SÄRTRYCK FRÅN STRATEGISK UTBLICK 6

Det fullt uppkopplade samhället – vision som kräver strategiska vägval

Peter Stenumgaard

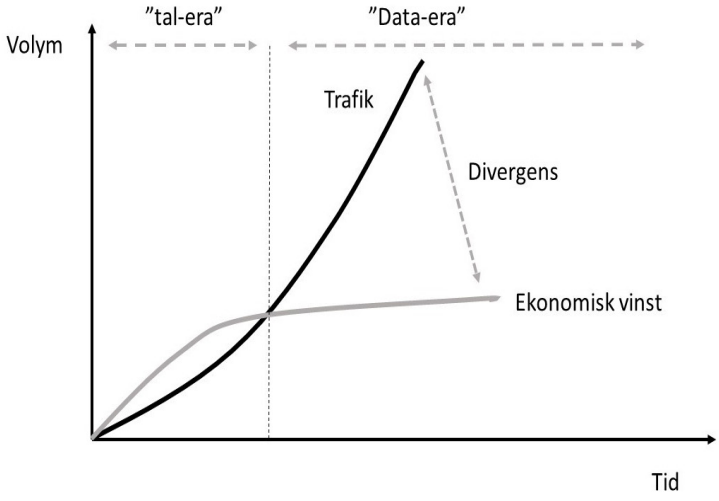
Antalet mobilabonnemang är idag ungefär lika stort som antalet människor på jorden. För att försäkra sig om fortsatt marknadstillväxt så arbetar mobilindustrin mot en vision som får dagens mobilanvändning att endast framstå som en början. Via ett massivt tekniksprång inom trådlös kommunikation, så ska efterföljaren till tredje (3G) och fjärde (4G) generationens mobilsystem – 5G – bana väg för det fullt uppkopplade samhället (eng. Networked Society) där trådlös teknik ska användas för att koppla ihop utrustning inom de flesta samhällssektorer. Hur kommer detta att påverka Sverige?

Sverige är en av de ledande nationerna i världen inom utvecklingen av 5G och detta paradigmskifte innebär avsevärt nya möjligheter till ekonomisk tillväxt. Samtidigt måste ett antal mycket viktiga strategiska vägval göras, både av myndigheter och näringslivsaktörer, för att hantera samhällets ökade sårbarhet och integritetsfrågor för medborgarna. Den massiva ökningen av trådlösa system kommer att öka sårbarheten både för angrepp med elektromagnetiska störningssignaler och för cyberattacker, då sådana angrepp kan utföras på avstånd från trådlösa system. På senare år har forskare visat både på möjligheter och risker med denna utveckling, båda kräver att viktiga strategiska vägval diskuteras.

Drivkrafter bakom visionen

I stort sett vart tionde år sker ett tekniklyft inom mobil kommunikation och en ny generation mobilsystem ser dagens ljus. Första generationen (1G) kom under 1980-talet, GSM (2G) under 1990-talet, 3G runt millennieskiftet. LTE (Long Term Evolution) kom runt 2010 och har utvecklats till 4G. Sverige har varit en av de ledande nationerna i världen vid den industriella utvecklingen av alla dessa generationers system och fortsätter att vara det även idag. Inför nästa generation är emellertid ambitionsnivån väsentligt högre och bågen är spänd för ett avsevärt tekniklyft.

Huvudskälet till mobilindustrins höga ambitioner för 5G kan förstås ur rent ekonomiska överväganden. Användningen av datatrafik ökar mycket snabbt både i handhållna enheter och bärbara datorer. Prognoser säger att den globala datatrafiken i mobilsystem kommer att växa mer än 200 gånger till 2020 och nästan 20000 gånger mellan 2010 och 2030. Av det skälet så krävs nya investeringar och uppgraderingar för att kunna möta det ökade behovet av datatrafik i mobila bredbandsnät. Teleoperatörerna står samtidigt inför en rad utmaningar relaterade till skalbarheten och kostnadsstrukturen i cellulära trådlösa nät. Dessa utmaningar måste hanteras för att kunna åstadkomma allt högre datatakter i näten. Samtidigt begränsar så kallade ”flatrate”-abonnemang (ett fast pris per månad för mobilt bredband) intäkterna då användarens kostnad för ett mobilabonnemang förblivit antingen konstant eller minskat de senaste åren. Detta har resulterat i ett fenomen som brukar benämnas vinstgap (eng. revenue gap), vilket visas schematiskt i figur 1.



Figur 1: Den ökande mängden datatrafik i mobila nät ökar snabbare än intäkterna från mobilabonnemang. Denna divergens leder till ett ”vinstgap”.

FOI-S--5402--SE
Godkänd av: Maria Lignell Jakobsson

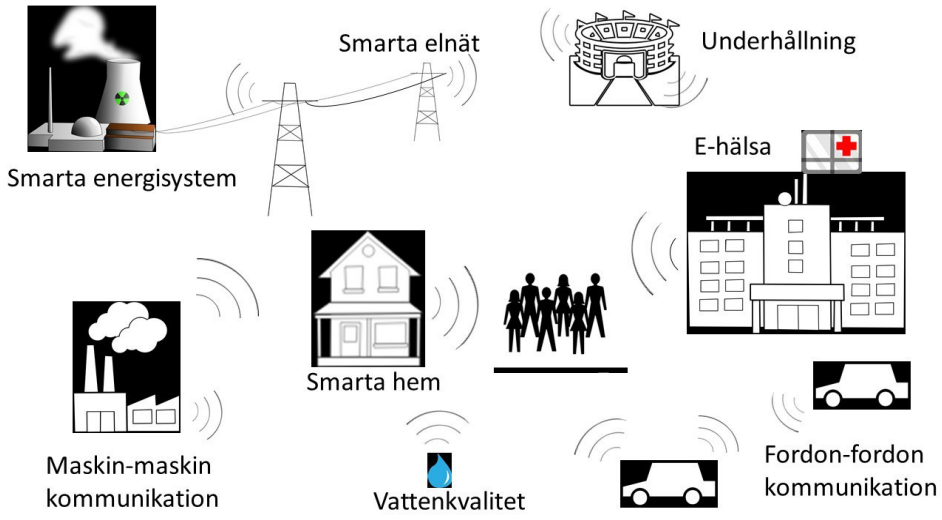
Särtryck ur Strategisk utblick 6
April 2016

Det behövs således ett nytt koncept för kostnadseffektiv och skalbar mobil infrastruktur för den ökande mängden mobil data, om marknaden ska kunna fortsätta att växa. Eftersom mängden mobilabonnemang som är möjlig att uppnå i världen dessutom begränsas av antalet människor på jorden, så måste nya tillämpningar för mobil bredbandskommunikation utvecklas. Målet framöver är därför att utrusta de flesta elektroniska system med trådlös internetuppkoppling. Genom att göra detta inom i princip samtliga samhällssektorer så skapas visionen om det fullt uppkopplade samhället. 5G utvecklas med målet att bli den första utvecklade infrastrukturen som är skalbar, mångsidig och energieffektiv för ett hyperuppkopplat ”Internet of Things”, IoT, (på svenska ung. ”sakernas internet”). Med IoT så avses att man kopplar upp annan elektronisk utrustning än sådan som vi människor bär med oss.

Idén att koppla upp elektronisk utrustning som inte hanteras av människor är inte ny i sig. Begreppet IoT har varit hett och diskuterats under flera år och innefattar i princip alla sorters elektroniska utrustningar i olika samhällssektorer. Än så länge är idén dock i praktiken fortfarande begränsad till olika enskilda isolerade initiativ, och IoT-applikationer är typiskt utvecklade som speciallösningar. Konsekvensen är ofta begränsad interoperabilitet mellan produkter utvecklade av olika aktörer eller för olika tillämpningsområden som exempelvis transport, energi eller ”smarta städer”. Vissa ser därför 5G som en teknisk nödvändighet för att IoT ska bli verklighet i full skala. 5G utvecklas som en grundförutsättning för den framtida digitala världen där en trådlös bredbandsinfrastruktur med ultrahög prestanda ska finnas tillgänglig inom alla ekonomiska sektorer och möta den ökade efterfrågan från konsumenter. Den trådlösa andelen av den globala internettrafiken förväntas växa från dagens ca 50 procent till runt 75 procent år 2020, då de första 5G-produkterna planeras bli tillgängliga på marknaden. Eftersom Sverige tillhör de världsledande nationerna inom telekommunikation har vi alltid varit tidiga användare av nya telekommunikationstjänster. Detta innebär att Sverige kommer att vara ett av de första länderna att uppleva de nya utmaningar som den massiva ökningen av trådlös teknik kommer att skapa för samhället. Vi står inför en situation som innebär både möjligheter och utmaningar. Genom att göra de rätta vägvalen kan Sverige dra fördel av möjligheterna snarare än att behöva kämpa utmaningarna.

Visionen för 5G

Visionen om det fullt uppkopplade samhället innefattar i princip samtliga samhällssektorer, se figur 2.



Figur 2: Visionen om det fullt uppkopplade samhället innefattar användningen av trådlös teknik inom de flesta samhällssektorer.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Tel: 08 5550 3000
Fax: 08 5550 3100
www.foi.se/strategiskutblick

Det finns mängder av exempel på 5G-tillämpningar såsom smarta städer, sjukvård, smarta hem, smarta elnät, jordbruk, intelligenta transportsystem (ITS), logistik, industristyrning, övervakning av miljö, utbildning, underhållning och medier. Potentialen anses vara så långtgående att somliga bedömare redan talar om en ny guldrush som möjliggörs av det fullt uppkopplade samhället. De tekniska målen för 5G är så ambitiösa att dagens systemprestanda kommer att överskridas avsevärt. Exempel är 10-100 gånger högre datatakt för den enskilde användaren, 1000 gånger mer mobil data per ytenhet (per användare), 10-100 ggr fler uppkopplade enheter samt tio gånger längre batteritid för kommunikation i maskintillämpningar med lägre effekter. Exempel på det senare är komponenter som sensorer där batteritiden kommer att vara upp till tio år. Samtliga dessa tekniska mål ska uppfyllas med en liknande kostnad och energiförbrukning per ytenhet som dagens cellulära system. 5G är följaktligen inte ett traditionellt evolutionärt utvecklingssteg av tidigare generations system; målet är snarare ett paradigmskifte. I det fullt uppkopplade samhället kommer flödet av information mellan enskilda enheter att öka dramatiskt på ett sätt vi inte upplevt tidigare.

Med nya tekniska möjligheter följer alltid nya utmaningar att handskas med och tekniska möjligheter är i sig inte det enda kriteriet som måste vara uppfyllt för att börja använda en enskild teknik. I detta fall krävs det att både samhällets sårbarhet och integritetsfrågor för individen måste hanteras i särskild ordning. Frågor om säkerhetsrisker och integritet leder därför till viktiga strategiska vägval som måste hanteras.

Sårbarhetsaspekter som kräver strategiska val

Trådlös teknik ökar i sig sårbarheten jämfört med trådbundna lösningar. Avsiktliga angrepp mot trådlösa system kräver inget tillträde till den direkta fysiska placeringen av ett system, utan kan utföras på avstånd. Följaktligen så kan cyberangrepp som varit möjliga att utföra i trådbundna nät utföras på ett bekvämt avstånd från ett trådlöst system. Eftersom alla trådlösa system är konstruerade för att ta emot begränsade signalnivåer kan de blockeras genom att helt enkelt sända en starkare signal i det rätta frekvensbandet. Civila trådlösa system är generellt sett inte robusta mot sådana störningssignaler, och åtgärder för att förbättra robustheten medför i regel stora kostnader.

Trådlösa system kan angripas på flera olika sätt; avsiktlig störning i syfte att blockera trafiken (eng. Denial of Service, DoS), avlyssning i syfte att extrahera information ur signalen, samt vilseledning i syfte att manipulera signalen med falsk information. Det är av avgörande betydelse att ta hänsyn till samtliga dessa hot i förväg så att inte prioriterade samhällskritiska tjänster blir beroende av sårbar trådlös teknik som är lätt att angripa. Kriminella utnyttjar redan idag sådana sårbarheter och medier rapporterar av och till om hur exempelvis störsändning används i samband med stölder och inbrott.

Ett exempel på hur en vanlig produkt utrustad med trådlös anslutning kan öka sårbarheten för ett cyberangrepp nämndes av USA:s tidigare vicepresident Dick Cheney när han den 20 oktober 2013 intervjuades i CBS program 60 minutes. Han berättade då att hans oro för att terrorister skulle kunna hacka sig in i hans pacemaker blivit så stor att han tidigare sett till att den trådlösa anslutningen avinstallerades. Säkerhetsexperten Barnaby Jack demonstrerade på konferensen BreakPoint Security Conference i Melbourne hur han kunde använda den trådlösa anslutningen för att få pacemakern att avge en elektrisk stöt på 830 Volt. Tidigare i år visade de två säkerhetsforskarna Charlie Miller och Chris Valasek hur de kunde ta över en bil via en trådlös anslutning. Genom att hacka sig in i en Jeep Cherokee från 2014 så kunde de påverka bilens styrning, slå av bromsarna och stänga av motorn. Senare återkallade Fiat Chrysler 1,4 miljoner fordon för att uppdatera programvaran. Ett annat exempel är säkerhetsforskarna Runa Sandvik och Michael Auger som i somras visade hur ett fjärrstyrt prickskyttegevär från TrackingPoint kunde hackas på avstånd. Med denna metod kunde de få geväret att skjuta på fel mål samt förhindra avfyrning. I en verklig situation skulle således användaren i praktiken tappa kontrollen över vapnet.

Även om ovanstående fall endast utgör ett fåtal exempel som är möjliga redan idag, så indikerar de hur en snabb och massiv ökning av trådlös internetteknik öppnar för ett nytt och komplext säkerhetshot. The

European Cybercrime Centre, EC3 (inom Europol) förutspår generellt fler dedikerade angrepp på existerande och kommande infrastruktur. Dessa angrepp inkluderar stöld av data och utpressning, såsom ransomware. Ransomware är en typ av skadlig programvara som infekterar ett system (exempelvis ett smart fordon eller smart hem) och begränsar användningen tills en lösensumma är betald. Förutom ekonomisk skada så kan även personskada bli en följd av sådan användning.

Tilltro kommer att bli, och måste vara, den nödvändiga basen för det fullt uppkopplade samhället. Tilltron behöver underbyggas av säkerhet och integritetsskydd. Utan det kommer sårbarheten hos samhällskritiska tjänster att öka samtidigt som industrin inte kommer att kunna nyttja den fulla affärspotentialen hos dessa nya möjligheter. Ett av flera strategiska val som måste göras är att besluta om vilka prioriterade samhällskritiska tjänster som skall vara anslutna till internet överhuvudtaget. Att låta övervakningssystem, system för insatspersonal, gränskontrollsystem, energisystem, trafikledningssystem eller vattenförsörjningssystem vara en del av det fullt uppkopplade samhället ökar sårbarheten för avsiktliga angrepp. Ett viktigt strategiskt val kan vara att helt exkludera vissa högprioriterade system från internetanslutning. Ett liknande val handlar om vilka samhällskritiska tjänster som skall tillåtas vara trådlöst förbundna med internet, eftersom det innebär att både cyberangrepp och avsiktlig störning kan göras på avstånd från systemen. Ett möjligt val skulle kunna vara att enbart tillåta trådlös anslutning till prioriterade samhällskritiska tjänster inom kontrollerade geografiska områden där endast auktoriserad personal har tillträde.

Visionen om det fullt uppkopplade samhället syftar till att göra våra vardagsliv enklare samtidigt som effektiviteten och produktiviteten kan öka i näringslivet. Den ökade mängden data kan hjälpa oss att göra val och fatta beslut men den kommer även att påverka våra förväntningar på personlig integritet. Om data som samlas in av olika system börjar användas på ett felaktigt sätt så kommer tilltron att undermineras. Information om energikonsumtionen i ett hem, teknisk status på hemelektronik med mera kan inte enbart komma att användas i kommersiellt syfte utan även av kriminella för att exempelvis ta reda på om någon är hemma. Ett annat exempel kan vara hur de etiska aspekterna av data kopplade till hälsostatus och som skickas via trådlösa armband ska hanteras.

Det måste vara tydligt för vardagskonsumenten hur användningen av data regleras med hänsyn till integritets- och etiska aspekter. Utan en sådan tydlighet, kan det bli svårt att få vardagskonsumenten att bli en entusiastisk användare av de nya tjänsterna i det fullt uppkopplade samhället. Detta gäller särskilt inom Europa, där tidigare forskning inom IoT-relaterade områden indikerat att integritetsaspekter är mycket viktiga. Eftersom Sverige är ett av de ledande länderna i arbetet med denna vision så är det rimligt att anta att detta paradigmskifte kommer att inträffa tidigt jämfört med många andra länder. Åter detta ger oss stora möjligheter att inte enbart skydda vårt samhälle från de sårbarheter som 5G-utvecklingen innebär, men även att dra nytta av de fördelar som det innebär att tillhöra de världsledande länderna inom området.

Internet är inte säkert idag, så vi kan inte förvänta oss att det fullt uppkopplade samhället blir säkert heller. Säkerhet utvecklas emellertid hela tiden för att möta nya utmaningar och medvetenheten om internetsäkerhet är stark bland ansvariga myndigheter i Sverige. Myndigheten för samhällsskydd och beredskap (MSB) har nyligen, tillsammans med Försvarsmakten, Försvarets radioanstalt samt Rikskriminalpolisen publicerat rapporten *Informationssäkerhet - trender 2015* (MSB779), som innehåller konkret stöd i det säkerhetsarbete som måste bedrivas i alla delar av samhället och för allas arbete med informations- och cybersäkerhet. I rapporten tas sju trendområden upp och en övergripande bild av situationen på informationssäkerhetsområdet beskrivs. Den kommande massiva ökningen av trådlös teknik i det fullt uppkopplade samhället kommer ytterligare att öka komplexiteten och sårbarhetsriskerna och därmed resultera i ytterligare utmaningar både inom internetsäkerhet och elektromagnetiska störningssignaler.

För att maximera möjligheterna och minimera sårbarheterna inom det fullt uppkopplade samhället så är det av största vikt att genomtänkta strategiska

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Tel: 08 5550 3000
Fax: 08 5550 3100
www.foi.se/strategiskutblick

vägval görs i god tid då komplexiteten i det kommande teknikspranget är så stor att det kan bli mycket svårt att åtgärda uppkomna sårbarheter med ad hoc-lösningar i efterhand. Frågor om i vilken grad prioriterade samhällskritiska tjänster ska vara anslutna till det fullt uppkopplade samhället samt hur den massiva ökningen av information som kommer att finnas tillgängliga i dessa nät ska hanteras måste avgöras i förväg om vi vill undvika ett sårbart samhälle med låg tilltro från användarna. Visionen om det fullt uppkopplade samhället torde erbjuda de största möjligheterna, men även de största utmaningarna med hänsyn till säkerhet och integritet, än något tidigare teknikspång i vårt samhälle.

Peter Stenumgaard

Strategisk utblick 6 finns att ladda ned från
www.foi.se/strategiskutblick

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Tel: 08 5550 3000
Fax: 08 5550 3100
www.foi.se/strategiskutblick