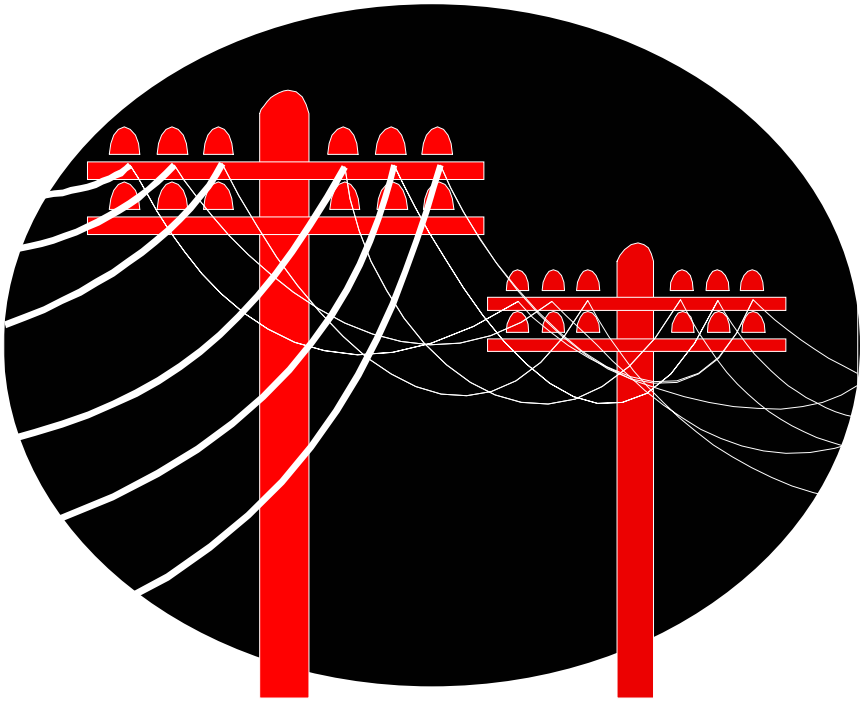
FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--1227--SE
April 2004
ISSN 1650-1942
**Användarrapport**

Göran Franzén, Svante Barck-Holst, Georg Fischer

# Telekommunikationernas sårbarhet och risker för samhället



SÄKRING AV VIKTIG INFRASTRUKTUR

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Försvarsanalys
172 90 Stockholm

FOI-R--1227--SE

April 2004

ISSN 1650-1942

**Användarrapport**

Göran Franzén, Svante Barck-Holst, Georg Fischer

# Telekommunikationernas sårbarhet och risker för samhället

| Utgivare | Rapportnummer, ISRN | Klassificering |
|---|---|---|
| Totalförsvarets Forskningsinstitut - FOI | FOI-R--1227--SE | Användarrapport |
| Försvarsanalys | **Forskningsområde** | |
| 172 90 Stockholm | 1. Försvars- och säkerhetspolitik | |
| | **Månad, år** | **Projektnummer** |
| | April 2004 | E1821, E1740 |
| | **Verksamhetsgren** | |
| | 5. Uppdragsfinansierad verksamhet | |
| | **Delområde** | |
| | 13 Stöd till säkerhet och beredskap | |

| Författare/redaktör | Projektledare |
|---|---|
| Göran Franzén | Svante Barck-Holst |
| Svante Barck-Holst | **Godkänd av** |
| Georg Fischer | Britt-Marie Lundholm |
| | **Uppdragsgivare/kundbeteckning** |
| | PTS |
| | **Tekniskt och/eller vetenskapligt ansvarig** |
| | Svante Barck-Holst |


**Rapportens titel**

Telekommunikationernas sårbarhet och risker för samhället


**Sammanfattning (högst 200 ord)**

Denna rapport redovisar den första fasen av en utredning för Post & Telestyrelsen avseende elektronisk kommunikation. Utredningen i sin helhet syftade till att föreslå en strategi för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Rapporten beskriver olika system för telekommunikation, vilka sårbarheter dessa system har samt hot som kan påverka dessa system. Dessutom ges exempel på risker för samhället vid bortfall av elektronisk kommunikation.

I rapporten konstateras bland annat att:

- Verksamheter beroende av elektronisk kommunikation själva måste vidta åtgärder för god säkerhet i denna.
- Det finns en stor känslighet för samtidiga störningar.
- Det fysiska skyddet för centrala noder i telefonisystemen är gott.
- På vissa ställen är det fysiska skyddet mindre väl utbyggt och stamnätets kablar är förhållandevis oskyddade.
- Det finns många operatörer och alternativa kanaler vilket bidrar till ökad säkerhet.
- En insider skulle kunna åstadkomma stor skada.
- Det ömsesidiga beroendet mellan systemen för elförsörjning och telekommunikation är en påtaglig riskfaktor.
- De informationstekniska hoten har tillfört en ny sårbarhetsdimension.



**Nyckelord**

Telekommunikationer, elektroniska kommunikationer, sårbarhet, risk

| Övriga bibliografiska uppgifter | Språk Svenska |
|---|---|
| | |
| **ISSN** 1650-1942 | **Antal sidor:** 65 s. |
| **Distribution enligt missiv** | **Pris: Enligt prislista** |

| Issuing organization | Report number, ISRN | Report type |
|---|---|---|
| FOI – Swedish Defence Research Agency<br>Defence Analysis<br>SE-172 90 Stockholm | FOI-R--1227--SE | User report |
| | **Programme Areas**<br>1. Defence and Security Policy | |
| | **Month year**<br>April 2004 | **Project no.**<br>E1821, E1740 |
| | **General Research Areas**<br>5. Commissioned Research | |
| | **Subcategories**<br>13. Support to Security, Safety and Preparedness | |



| Author/s (editor/s) | Project manager |
|---|---|
| Göran Franzén<br>Svante Barck-Holst<br>Georg Fischer | Svante Barck-Holst |
| | **Approved by**<br>Britt-Marie Lundholm |
| | **Sponsoring agency**<br>PTS |
| | **Scientifically and technically responsible**<br>Svante Barck-Holst |


**Report title (In translation)**

Vulnerability of Telecommunications and Risks for Society


**Abstract (not more than 200 words)**

The Government commissioned the National Post and Telecom Agency (PTS) to present a strategy for the tele-communications-sector to reduce consequences for society of severe peacetime emergencies and increase the preparedness to face a state of national alert and war.

This report presents the results of the first phase of this work. It describes different systems for telecommunications as well as the vulnerabilities and threats affecting these systems. Examples of consequences for society caused by loss of telecommunications are also given. In the report it is concluded that:

- Organisations depending on electronic communication must take precaution to ensure the security of their own communications.
- There is a high degree of sensitivity to simultaneous disturbances.
- The physical protection of central nodes in the telecommunication systems is good.
- In some places and for cables of the network backbone the physical protection is less developed.
- There are many operators and alternative forms of electronic communication which gives increased security.
- An insider could cause considerable damage.
- Mutual dependencies between power supply and telecommunications are evident risk-factors.
- Computer network attacks have added a new dimension to the issue of vulnerability.



**Keywords**

Telecommunications, electronic communications, vulnerability, risk

| Further bibliographic information | Language Swedish |
|---|---|
| | |
| **ISSN** 1650-1942 | **Pages** 65 p. |
| | **Price acc. to pricelist** |

# Förord

Totalförsvarets forskningsinstitut - FOI har till uppgift att bedriva forskning, metod- och teknikutveckling samt utredningsarbete till stöd för totalförsvaret och till stöd för nedrustning och internationell säkerhet. I ökande utsträckning bedriver FOI även forsknings-, utrednings- och utvecklingsarbete för civila kunder utanför totalförsvaret. Verksamheten skall bedrivas med beaktande av krav på relevans, integritet, vetenskaplig kvalitet och effektivitet.

Denna rapport färdigställdes för Post & Telestyrelsen, PTS, som en första del i en utredning avseende elektronisk kommunikation. Utredningen i sin helhet syftade till att föreslå en strategi för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Vid Totalförsvarets forskningsinstitut, FOI, bedrivs sedan 2000 det av Krisberedskapsmyndigheten finansierade ramforskningsprogrammet ”Säkring av viktig infrastruktur”. Ramforskningsprogrammet syftar till att skapa en långsiktig kunskapsuppbyggnad och till att upprätthålla en hög kompetensnivå rörande säkringen av viktig infrastruktur. Syftet med ramprogrammet är att utveckla kunskaper och bygga upp kompetens om såväl de fysiska infrastrukturerna som de överlagrade informationsinfrastrukturerna. Programmet är inriktat mot att skapa grundläggande kunskaper om infrastruktursystem, infrastrukturernas interna och externa beroendeförhållanden, hotbilden mot vital infrastruktur, sårbarheter i och konsekvenser av störningar i infrastruktursystem samt möjliga åtgärder för att säkra vital infrastruktur. Denna utredning rörande de elektroniska kommunikationerna ligger nära kärnan i verksamheten för ramprogrammet och en del av utredningsarbetet har därför finansierats inom ramprogrammet. Detta har gett utrymme för en betydande fördjupning i arbetet med utredningen.

Rapporten har författats av tekn. lic. Göran Franzén, BDO Consulting Group Stockholm AB, civiling. Svante Barck-Holst, Forskare på FOI, och Georg Fischer, 1:e Forskare på FOI. Arbetet har skett i samarbete med PTS och med visst underlag från teleoperatörer.

Rapporten levererades till PTS i september 2002 (PTS diarienummer 02-12281). I mars 2003 avslutades utredningen med slutrapporten ”Robusta elektroniska kommunikationer, Strategi för åren 2003-2005” (PTS rapport PTS-ER-2003:13).

Författarna vill tacka samtliga som har bidragit med underlag och synpunkter till denna studie. Ett särskilt tack riktas till de personer som ställt upp med sin tid och kunskap i de intervjuer som genomförts. Ett särskilt tack riktas även till Ulf Pettersson, Nätsäkerhetschef vid Teracom, som vid den slutliga granskningen av rapporten i december 2003, bidragit med konstruktiv kritik.

Svante Barck-Holst
Projektledare vid FOI

# Innehållsförteckning

# Sammanfattning

Denna rapport redovisar den första fasen av en utredning avseende elektronisk kommunikation. Utredningen i sin helhet syftar till att föreslå en strategi för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Vi diskuterar i denna delrapport tänkbara hot mot olika former av elektronisk kommunikation, kommunikationernas sårbarhet i tekniskt avseende samt risker för samhället av störningar i de elektroniska kommunikationerna.

## *Hoten*

Som svåra påfrestningar på samhället betraktar vi situationer där det uppstått allvarliga störningar i viktiga samhällsfunktioner och där det behövs samordnade insatser från flera olika myndigheter och organ för att kunna hantera situationen och därmed begränsa konsekvenserna. Sådana situationer kan t.ex. utvecklas ur extremt väder, svåra olyckor, omfattande och långvariga avbrott i den tekniska infrastrukturen eller terroristangrepp. Även om det internationella säkerhetspolitiska läget förbättrats går det inte att utesluta att begränsade angrepp, med olika påverkansmedel, riktas mot Sverige i samband med en kris som utvecklas ur nuvarande omvärldsläge.

Teknisk infrastruktur, t.ex. elförsörjning och telekommunikationer, spelar en allt viktigare roll för att kunna upprätthålla samhällets vitala funktioner. Sårbarheten i dessa system och den informationstekniska utvecklingen har inneburit att även mindre intressegrupper, ekonomiskt svagare stater, terrorister och kriminella grupper fått större möjligheter att påverka, oavsett var i världen de befinner sig. Detta förhållande innebär att motståndsförmågan blir alltmer beroende av samhällsutvecklingen och risken ökar för att även en angripare med stora militära resurser väljer att i första hand rikta sina angrepp mot den civila infrastrukturen.

Det finns således såväl i fredstid som vid höjd beredskap och krig tänkbara hot mot de elektroniska kommunikationerna. För att bedöma sårbarheten finns det skäl att skilja på slumpmässiga och avsiktliga hot. För att allvarliga störningar skall uppstå fordras ofta att flera funktioner, delsystem eller fysiska anläggningar drabbas samtidigt. Eftersom slumpmässiga, oavsiktliga och oberoende hot sällan inträffar samtidigt går det relativt lätt att skydda de elektroniska kommunikationerna mot sådana genom reserver och redundanta nät. Den avsiktlige aktören däremot kan alltid förväntas söka agera så att samtidiga insatser mot olika mål förstärker varandra.

Slumpmässiga hot kan främst bedömas uppstå vid extremt väder och på grund av tekniska fel, felaktig hantering och olyckor. Avsiktliga hot kan utövas genom fysisk påverkan som avklippning av kablar eller förstöring av utrustning. Men de kan också utövas med informationstekniska medel. Intrång i datasystem av olika slag via teleförbindelser eller Internet kan göras för att manipulera dem och störa t.ex. elförsörjning, telesystem och betalningar.

## *Den tekniska sårbarheten*

I rapporten diskuterar vi den tekniska sårbarheten hos fasta telenät, mobila telenät, nät för datakommunikation, IT-infrastruktur med hög överföringskapacitet samt de elektroniska kommunikationernas beroende av el. Vi belyser också utvecklingen mot allt större integration mellan olika typer av elektronisk kommunikation.

Elektronisk kommunikation sker i regel från en terminal genom ett accessnät till en uppsamlingspunkt. Informationen flyter sedan genom ett transportnät för att till sist via ett accessnät föras till en annan terminal. Accessnäten i det fasta telenätet är sårbara. De består i regel av kopparledning fram till abonnenten och är utsatta både för fysisk påverkan och väder och vind. Redundansen i det fasta accessnätet är låg och enstaka störningar får därför direkt effekt.

Transportnäten består främst av optisk fiber. De är ofta gemensamma mellan olika typer av elektronisk kommunikation och har mycket högre kapacitet än accessnäten. Avbrott i transportnäten berör därför många abonnenter. På denna nivå i näten blir det därför viktigt med redundans. Näten innehåller växlar men också speciella noder för att hantera intelligenta tjänster och speciella databaser. Det är viktigt att skydda olika typer av noder mot åverkan och intrång.

Skillnaden mellan det mobila och det fasta nätet är huvudsakligen att mobilnätets accessnät är trådlöst och att det mobila nätet behöver funktionalitet för att lokalisera och identifiera abonnenterna. Basstationerna utgör en relativt oskyddad del i de mobila telenäten. Vid bortfall av en enstaka sådan påverkas dock i regel snarare kapaciteten än täckningen.

Tele- och datanäten är helt beroende av el för att fungera. Avbrott i elförsörjningen på upp till ett par timmar klarar man normalt då de flesta noder i telenäten är försedda med batteri-backup. Centrala noder klarar sig normalt ännu längre då de dessutom ofta har reservkraft i form dieselgeneratorer. Ett av de vanligaste problemen anges av operatörerna dock vara elavbrott.

## *Risker för samhället vid bortfall av elektronisk kommunikation*

Elektronisk kommunikation spelar idag en omfattande roll för i stort sett alla samhällsfunktioner. En fullständig eller samlad bild är svår för att inte säga omöjlig att sammanställa. Man kan dock konstatera att beroendet är stort och att det hela tiden ökar. Bortfall av elektroniska kommunikationer kan därför medföra stora risker för samhället.

Näringsliv och myndigheter använder sig i stor utsträckning av telefon, fax, Internet och e-post för att kommunicera internt och externt. Man använder sig av mobiltelefon för att kommunicera med personal som jobbar ”ute på fältet”. Fax och e-post används för att diskutera, informera och kommunicera. Internet används för att nå en bredare publik med information. Man har så kallade intranät för att informera den egna personalen och externa nät, oftast Internet, för att informera sina kunder/medborgare.

Många företag har idag datoriserade order-, lager- och faktureringssystem som är direkt beroende av fungerande telekommunikationer.

Sveriges betalningssystem är mycket beroende av fungerande tele- och datakom-munikationer. De olika aktörerna i betalningssystemet överför varje dag mycket stora belopp mellan varandra. Detta datautbyte sker till största delen via fiber som man hyr av teleoperatörerna. Likaså sker en stor del av betalningarna i handeln numera via betalkorts-terminaler som är beroende av de publika telenäten.

Ett enstaka avbrott i elektroniska kommunikationer under begränsad tid leder normalt inte till en svår påfrestning på samhället. Det kan dock få svåra följder om en viktig samhällsfunktion drabbas eller om avbrottet inträffar i en svår kris. Störd elektronisk kommunikation kan få svåra konsekvenser för exempelvis industriell verksamhet, handel och betalningsväsende. Erfarenheter från långvariga störningar i Kanada och Nya Zeeland pekar på den stora betydelsen av väl förberedd förmåga till krishantering. Några exempel på viktiga samhällsområden som är beroende av god elektronisk kommunikation vid kriser är SOS Alarm, räddningstjänsten, ledning från central nivå, kommuner och landsting,

polisen, sjukvården, elförsörjningen och media. Vid höjd beredskap och krig är totalförsvarets elektroniska kommunikationer av avgörande betydelse.

## *Samlad värdering*

Sverige har en lång tradition av att inom totalförsvarets ram skapa säkra telekommunikationer. Nu har emellertid hotbilden förskjutits och ställt inte minst svåra fredstida påfrestningar i fokus. Det senaste decenniets avreglering och kommersialisering av telemarknaden i kombination med den snabba utvecklingen av mobil telefoni och datakommunikation har inneburit stora förändringar. Behovet av säkra kommunikationer har ökat liksom möjligheterna att tillgodose detta. Det finns därför anledning att kritiskt pröva säkerheten i dagens system för telekommunikationer och vad vi bygger för framtiden.

Alla verksamheter som är beroende av elektronisk kommunikation måste ta ansvar för sin egen vardagssäkerhet. Därigenom skapas en basförmåga och en grundläggande robusthet och beredskap att motstå hot och hantera störningar. Denna basförmåga utgör en nödvändig grund och förutsättning för att samhället skall ha tillfredsställande telekommunikationer också vid svåra påfrestningar i fred och vid höjd beredskap och krig.

Det måste ställas ett grundläggande krav på samhällsviktiga funktioner att inom ramen för sin ordinarie verksamhet vidta åtgärder för att skapa god säkerhet i telekommunikationerna redan vid normalt förekommande störningar. Det kan ofta ske med enkla medel genom att t.ex. ha lokal reservkraft, anlita flera operatörer, använda flera fysiskt skilda anslutningar till telenäten och att skapa lokala skydd mot dataintrång och fysiska intrång. Den allmänna bild vi fått av vardagssäkerheten inom dessa samhällsviktiga områden är inte odelat positiv.

Den basförmåga av säker elektronisk kommunikation som finns i samhället tillgodoser dock totalt sett ganska höga krav på säkerhet för samhällets funktion vid enskilda störningar under normala förhållanden. Vad som kan ge större problem för de elektroniska kommunikationerna och för samhällets funktion är när flera störningar inträffar samtidigt. Det kan t.ex. ske vid väderstörningar i större områden, när någon annan större påfrestning som ett längre elavbrott eller stor olycka slår ut elektroniska kommunikationer med förstärkta svårigheter som följd eller när någon avsiktlig aktör samtidigt påverkar flera funktioner så att redundansen reduceras och reservmöjligheter försvinner.

Det fysiska skyddet för centrala noder i stamnätet och centrala styrnoder för både fast och mobil telefoni är gott. Mer tveksamt är om skyddet mot informationsintrång är lika gott och kommer att förbli det när integrationen av fast tele, mobil tele och datatrafik ökar och informationsvägarna blir alltmer komplexa. Vi noterar dock att avsevärda försiktighetsåtgärder företas för att förhindra intrång i styrnäten.

På medelhög nivå i näten är det fysiska skyddet mindre utbyggt även om noder i regel finns i utrymmen med tillträdesskydd. Stamnätets kablar är förhållandevis oskyddade även om de är nedgrävda. När antalet fysiskt åtskilda vägar för informationsflödet är litet, som till Norrland och till Gotland, kan en sabotör som lyckas lokalisera kablarna relativt enkelt åstadkomma totala avbrott i förbindelserna.

En faktor som bidrar till ökad säkerhet är att det numera finns ganska många operatörer och att mobil telefoni och datakommunikation i separata kanaler blir allt vanligare. Samtidigt kan dock flera förbindelser i något led vara beroende av en och samma del av stamnätet eller av någon central styrfunktion.

Den inre säkerheten hos olika operatörer men också hos användarna av elektronisk kommunikation får allt större betydelse. En så kallad insider skulle kunna åstadkomma stor skada genom att utnyttja sin kunskap och sina möjligheter till tillträde för att skada de

elektroniska kommunikationerna. Tillgång till insiderkunskap är viktig också för den yttre sabotör som vill orsaka störningar genom att klippa av kablar eller förstöra knutpunkter. Det är därför väsentligt för säkerheten att begränsa möjligheterna till insyn och påverkan från egen personal, inhyrda entreprenörer eller samverkande parter. Särskilt viktig är den inre säkerheten när det gäller systemuppbyggnad, stamnät och styrfunktioner.

Ett påtagligt riskområde är det ömsesidiga beroende mellan systemen för elförsörjning och telekommunikation. Väderstörningar drabbar ofta samtidigt både elförsörjning och telekommunikationer och kan få en varaktighet som gör batterireserver otillräckliga. De samlade systemen för elförsörjning och telekommunikation kan även bedömas utgöra intressanta mål för terrorister, sabotörer eller militära insatser mot mål i Sverige. Även om de mest centrala noderna är skyddade finns många möjligheter till påverkan med relativt enkla medel för den som har tillräcklig kännedom om systemens uppbyggnad. De reserver som finns är knappast dimensionerade för sådana extrema situationer.

De informationstekniska hoten har tillfört en ny dimension till de elektroniska kommunikationernas sårbarhet och därmed förknippade risker. Det handlar inte längre bara om att ha tillgång till en förbindelse med tillräcklig kapacitet utan också om att kunna lita på riktigheten såväl av den uppkopplade förbindelsen som av den information som överförs. Det gör det nödvändigt att beakta inte bara kommunikationernas uthållighet och tillgänglighet utan också deras tillförlitlighet. De åtgärder som vidtas för att allmänt öka IT-säkerheten i samhället har stor relevans också för de elektroniska kommunikationernas tillförlitlighet.

De elektroniska kommunikationerna har kommit att bli alltmer gränsöverskridande till sin karaktär. Säkerheten i datakommunikationer är sedan länge ett utpräglat internationellt problem. Elektronisk kommunikation i Sverige blir därmed beroende av hur väl kommunikationssystemen skyddas och fungerar i andra länder. Även om vi söker finna inhemska lösningar för säkerhet i elektroniska kommunikationer vid svåra påfrestningar på samhälle i fred, höjd beredskap och krig, kommer säkerheten också att vara beroende av ett internationellt samarbete.

Vi har under arbetets gång funnit att det finns anledning att vid en genomgång av telekommunikationernas sårbarhet och risker för samhället också ta med distribution av ljudradio och TV i bilden. Detta har dock inte gjorts i denna delrapport.

## *Fortsatt arbete*

Det fortsatta utredningsarbetet skall leda fram till en strategi för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig. Vid värdering av olika åtgärder måste man ta hänsyn till såväl kostnader för åtgärderna som bedömd nytta av dem. Åtgärder som övervägs bör väljas och värderas mot bakgrund av i denna delrapport redovisade risker och sårbarheter. Exempel på sådana åtgärder kan vara att granska säkerheten hos samhällsviktig verksamhet, att bidra till att förbättra fysiskt och elektroniskt skydd, att öka nätverkens flexibilitet och redundans, att stärka elförsörjningen, att förbättra IT-säkerheten, samt att öva och utveckla möjligheter till krishantering.

# 1 Inledning

## 1.1 Uppdraget

Regeringen har givit PTS i uppgift att för telekommunikationerna redovisa en strategi för hur arbetet med åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och med att öka beredskapen inför höjd beredskap och krig skall bedrivas. Strategin skall avse åren 2003 t.o.m. 2005. Som en grund för strategin skall en risk- och sårbarhetsanalys genomföras. Härvid skall särskilt redovisas en strategi för säkerhetsarbetet avseende noder och redundans i IT-infrastruktur med hög överföringskapacitet och en strategi för samplanering mellan berörda myndigheter avseende beroenden mellan el- och telesystem vid omfattande och långa elavbrott. Uppdraget skall redovisas till regeringen med en delrapport senast den 1 oktober 2002 och med en slutrapport senast den senast den 1 april 2003.

PTS har för att genomföra uppdraget tagit hjälp av konsulter. Denna delrapport har utarbetats av konsulterna i samverkan med PTS och FOI:s institution för system- och funktionsvärdering och med visst underlag från teleoperatörer. Författare är tekn. lic. Göran Franzén, BDO Consulting Group Stockholm AB och civiling. Svante Barck-Holst, Totalförsvarets forskningsinstitut, FOI. I utredningsarbetet har även Georg Fischer, 1:e Forskare på FOI, tagit aktiv del.

## 1.2 Tolkning av uppdraget

Vi tolkar uppdraget som att det skall avse en strategi för val och prioritering av åtgärder som staten under åren 2003 t.o.m. 2005 bör vidta för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig. Syftet med åtgärderna skall vara att minska risken för att samhället utsätts för svåra påfrestningar, att minska konsekvenserna av situationer där samhället utsätts för svåra påfrestningar i fred samt att öka beredskapen inför höjd beredskap och krig. Strategin bör avse principer för hur tillgängliga medel bör fördelas på olika säkerhetshöjande insatser men bör också, om det befinns lämpligt, kunna avse andra typer av åtgärder t.ex. förändringar i det statliga regelsystemet för den berörda verksamheten eller formerna för samarbete mellan berörda myndigheter och privata aktörer på området.

Åtgärderna bör syfta till att höja säkerheten i såväl ett kortsiktigt som längre perspektiv. Kortsiktigt kan det t.ex. handla om att avhjälpa akuta brister eller att upprätthålla en viss beredskap att hantera störningar. Långsiktigt kan det t.ex. handla om investeringar i en robustare och mindre störningskänslig infrastruktur eller om forskning och utveckling för att kartlägga hot och risker och finna möjligheter att öka säkerheten. Kortsiktigt bestäms tänkbara hot mot telekommunikationerna av det aktuella läget i omvärlden och av dagens system för telekommunikationer. På längre sikt finns det anledning att beakta också möjligheten av ett bredare spektrum av hot och av utvecklade metoder och medel för telekommunikation.

Uppdraget avser svåra påfrestningar på samhället i fred samt höjd beredskap och krig. Det innebär att konsekvenserna av tänkbara störningar i telekommunikationerna bör vara av en viss dignitet för att de skall beaktas inom ramen för uppdraget. Vår utgångspunkt är att söka finna lösningar som gör det möjligt att i de situationer som uppdraget avser upprätthålla en standard och kvalitet i telekommunikationerna som kan bedömas som rimlig i förhållande till den rådande situationen i stort i samhället.

Till området telekommunikationer räknar vi alla typer av elektronisk kommunikation för att överföra och utbyta information. Överföringen kan ske med traditionell analog teknik eller med digitaliserad teknik eller en kombination av dessa. Den kan ske i kopparledningar och -kablar, i optiska kablar och genom radiovågor. Utvecklingen går mot en konvergens mellan olika typer av elektronisk kommunikation där tal, bild och data i ökande utsträckning överförs i digitaliserad form i samma eller samverkande nät. För att behandla frågor om sårbarhet är det nödvändigt att se de alltmer konvergerande typerna av elektronisk kommunikation i ett helhetsperspektiv. Detta innebär även att vi i rapporten behandlar en mängd system för elektronisk kommunikation och inte begränsar oss till sådana system för vilka PTS har ett utpekat ansvar. Vi har under arbetets lopp kommit fram till åsikten att detta helhetsperspektiv i princip bör omfatta även distribution av ljudradio och TV. Vi går dock i denna rapport inte närmare in på frågor som rör dessa former av elektronisk kommunikation.

För att understryka den bredd vi lägger i begreppet telekommunikation använder vi i rapporten ofta begreppet elektronisk kommunikation. Vi vill därmed undvika en snäv associering till enbart konventionell kretskopplad telefoni.

De speciella frågorna i uppdraget om noder och redundans i IT-infrastruktur med hög överföringskapacitet samt beroenden mellan el- och telesystem vid omfattande och långa elavbrott understryker vikten av ett helhetsperspektiv. Stamnätet för elektronisk kommunikation tenderar att alltmer bli gemensamt för alla typer av sådan kommunikation och det ömsesidiga beroendet mellan el- och tele accentueras av den tekniska utvecklingen.

## 1.3 Principer för säker elektronisk kommunikation

Som utgångspunkt för vårt arbete har vi använt följande princip för hur samhället bör tillgodose sitt behov av säker elektronisk kommunikation under normala förhållanden respektive vid svåra påfrestningar på samhället i fred och vid höjd beredskap och krig:

Den snabbt ökande användningen av elektronisk kommunikation för att bedriva nästan all typ av verksamhet i samhället har gjort det till en nödvändighet att ständigt ha tillgång till snabb och tillförlitlig sådan kommunikation med hög kapacitet och säkerhet. Med den elektroniska kommunikationens hjälp kan de flesta verksamheter uppnå både hög funktionalitet och hög effektivitet. Den elektroniska kommunikationens stora nytta gör att användarna ställer höga krav på dess funktion och har ekonomiskt intresse av hög tillgänglighet och tillförlitlighet. Marknadsmekanismerna kan därför i vardagssamhället förväntas, i ett samspel mellan kunder och operatörer, påverka de satsningar som görs för att under normala förhållanden uppnå en hög säkerhet mot störningar som svarar mot den elektroniska kommunikationens betydelse.

Den elektroniska kommunikationens centrala roll i samhället gör att dess funktion blir en fråga av säkerhetspolitisk dignitet. Sedan mitten av 1990-talet har den säkerhetspolitiska synen vidgats och det kalla krigets invasionshot ersatts med en breddad hotbild. I säkerhetspolitiken ingår därför inte bara att möta väpnade angrepp utan även att förebygga och skapa en beredskap att hantera sådana situationer som utan att direkt hota landets fred och självständighet likväl kan innebära svåra påfrestningar på samhället. Mot denna bakgrund har en utveckling skett mot en helhetssyn på samhällets samlade förmåga att möta risker och kriser vid såväl svåra påfrestningar i fred som vid höjd beredskap och krig.

Det är tveksamt om marknadsmekanismerna ensamma förmår att skapa ett tillfredsställande skydd mot störningar i den elektroniska kommunikationen i extraordinära situationer av allvarlig art där viktiga samhällsfunktioner hotas eller när landet utsätts för angrepp. Det blir i stället en kollektiv uppgift för staten att komplettera det skydd och den

säkerhet som finns i vardagens elektroniska kommunikation med åtgärder för att öka säkerheten också vid mer sällsynta men ändå tänkbara allvarliga störningar. Dessa kompletterande säkerhetshöjande åtgärder kommer ofta att bidra till ökad säkerhet även under normala förhållanden. De har därmed också ett visst kommersiellt värde även om det inte är tillräckligt för att de skall komma till stånd på rent kommersiella grunder.

Ambitionen för de kompletterande åtgärderna kan rimligen inte vara att i alla avseenden vidmakthålla den grad av tillgänglighet och säkerhet som råder normalt utan bör begränsas till att säkerställa en till de extrema situationerna anpassad standard.

Vid svåra påfrestningar på samhället i fred handlar det då om att viktiga samhällsfunktioner som ledningsfunktioner, vård och omsorg, försörjning med livsmedel och vatten, distribution av samhällsviktiga varor, betalningsväsende, massmedial information etc. kan fungera åtminstone hjälpligt. Däremot kan det vara rimligt att acceptera t.ex. vissa avbrott i produktionen och att enskilda personer och företag lider vissa ekonomiska avbräck.

I en situation med hotande väpnat angrepp eller i krig begränsar sig anspråken på standard ännu mer till livsnödvändiga funktioner och till att möjliggöra ett effektivt försvar.

## *1.4 Utredningen om elektronisk kommunikation*

Som ett uttryck för samhällets samlade värdering av de elektroniska kommunikationernas betydelse har vi tagit de allmänna politiska mål som Utredningen om elektronisk kommunikation nyligen föreslagit i sitt delbetänkande[1]. Utredningen föreslår följande målsättning för elektronisk kommunikation grupperad på tre nivåer:

> ”Elektronisk kommunikation skall vara så effektiv att den främjar tillväxt, ökar svensk konkurrenskraft samt bidrar till ökad produktivitet i samhället. Elektronisk kommunikation skall även bidra till att målet för mediepolitiken uppnås, dvs. stödja yttrandefrihet, mångfald, massmediernas oberoende och tillgänglighet samt motverka skadliga inslag i massmedierna.
>
> Enskilda och myndigheter skall ha största möjliga tillgång till effektiva och säkra elektroniska kommunikationer med bästa möjliga urval, pris och kvalitet. Det främsta medlet att uppnå detta är en effektiv konkurrens. Politiken skall därför främja en konkurrens utan snedvridningar och begränsningar.
>
> Politiken för elektronisk kommunikation skall vidare säkerställa:
>
> - att enskilda och myndigheter har tillgång till grundläggande tjänster till överkomliga priser i hela landet
> - att grundläggande tjänster är tillgängliga på ett likvärdigt sätt, bl.a. för att tillgodose funktionshindrades behov
> - att enskilda har tillgång till nödtjänster
> - skydd av den personliga integriteten
> - uthållighet och tillgänglighet under svåra påfrestningar på samhället i fred, höjd beredskap och krig
> - ett effektivt utnyttjande av frekvenser och adresser
> - ett verkningsfullt konsumentskydd

[1] SOU 2002:60 Lag om elektronisk kommunikation

samt främja

- en hållbar utveckling mot en hälsosam och god miljö
- internationell harmonisering”

Främst sätts alltså effektivitet och samhällsnytta. Medlet för att nå detta är primärt fri konkurrens. Politiken skall därutöver säkerställa vissa specifika mål varav uthållighet och tillgänglighet under svåra påfrestningar på samhället i fred, höjd beredskap och krig utgör ett.

Utredningen föreslår alltså att de elektroniska kommunikationerna skall vara uthålliga och tillgängliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig. Utredningen konstaterar:

> ”Dagens regelsystem gäller enbart funktionssäkerheten i telesystemet under kris och krig. Den nya formuleringen innebär att alla elektroniska kommunikationer skall vara uthålliga och tillgängliga under sådana förhållanden.
>
> De elektroniska kommunikationerna bör dessutom vara uthålliga och tillgängliga under svåra påfrestningar i fred.”

Beträffande medel och metod att nå målen för säkerhet i den elektroniska kommunikationen gör utredningen följande kommentar:

> ”Dagens säkerhetskrav innebär enligt telelagen att den som inom ett allmänt tillgängligt telenät tillhandahåller teletjänster eller nätkapacitet skall se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet. Enligt målparagrafen (2§) syftar bestämmelserna till uthålliga telekommunikationer i fredstid och under kriser och krig. Detta tillgodoses på olika sätt i lagen. I det regelverk som föreslås är driftsäkerhet under normala förhållanden en fråga som överlämnas till marknaden. Krav kan dock ställas på samhällsomfattande tjänster. Finansieringen är idag delad eftersom operatörerna normalt inte anses ha behov av de krav en krigssituation ställer; däremot har de intresse av störningsfri drift i fredstid. Åtgärder mot allvarliga hot och påfrestningar i fredstid finansieras genom offentligrättsliga avgifter från operatörer med betydande inflytande på marknaden. Medlen redovisas mot inkomsttitel på statsbudgeten och motsvarande belopp anvisas som anslag. Övriga åtgärder inom funktionen telekommunikationer finansieras med medel från statsbudgeten. Vi ser inget behov av att öka statens insatser på området eller föreslå någon annan metod att uppnå målen inom detta område.”

## 1.5 Uppläggning av arbetet

Vi har delat in arbetet i två faser. Den första med delrapport i september 2002, behandlar de elektroniska kommunikationernas sårbarhet och risker för samhället. Den andra, med slutrapport i mars 2003, behandlar det samlade uppdraget att utforma en strategi för hur arbetet med åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och med att öka beredskapen inför höjd beredskap och krig skall bedrivas.

Den uppläggning vi valt för arbetet i den första fasen är att först skaffa en överblick genom att gå igenom tidigare utredningar och annat bakgrundsmaterial som vi bedömt ha relevans för frågeställningarna. I slutet av delrapporten finns en litteraturförteckning. Vi har sedan sökt strukturera och preliminärt analysera sårbarhet och risker.

I enlighet med propositionen om samhällets säkerhet och beredskap[2] värderar vi inte de elektroniska kommunikationernas sårbarhet enbart i sig utan söker beakta också vilka de tänkbara hoten är och i hur hög grad samhället är beroende av att kommunikationerna fungerar. Vår risk- och sårbarhetsanalys omfattar de tre stegen:

1. vilka hot som kan finnas mot de elektroniska kommunikationerna,
2. vilken teknisk sårbarhet som kommunikationssystemen har och
3. vilka risker för samhället som bortfall av kommunikationsförmåga kan medföra.

För att risken och sårbarheten samlat skall vara hög anser vi att produkten av de tre faktorerna i någon mening måste vara hög sett i relation till rimlig standard inom ramen för en svår påfrestning på samhället i fred eller vid höjd beredskap och krig.

Med vår preliminära analys som grund har vi inhämtat fördjupat underlag genom intervjuer med ett antal personer vid PTS och hos tele- och nätoperatörer med god kännedom om systemen för elektronisk kommunikation och med erfarenhet av säkerhetsfrågor. Totalförsvarets forskningsinstitut har vidare bidragit med erfarenheter och resultat från andra studier man genomfört om samhällets sårbarhet. Med detta ytterligare underlag som grund har vi sedan utvecklat vår preliminära analys till den mer genomarbetade analys av de elektroniska kommunikationernas sårbarhet och risker för samhället som redovisas i denna delrapport.

På grundval av risk- och sårbarhetsanalysen är avsikten att i en andra och avslutande etapp utforma en strategi för val och prioritering av åtgärder inom området elektronisk kommunikation för att minska risker och sårbarhet. Val mellan olika typer av åtgärder bör i princip göras mot bakgrund av deras kostnadseffektivitet för att reducera konsekvenserna för samhället av den samlade risken och sårbarheten hos de elektroniska kommunikationerna.

## *1.6 Arbetets genomförande*

Uppdraget med att ta fram föreliggande sårbarhetsanalys påbörjades i april 2002 och slutfördes i och med att en rapport[3] överlämnades till PTS i september 2002. Underlag till rapporten har inhämtats genom litteraturstudier och intervjuer.

Telekommunikationsområdet är stort, komplext, tekniskt avancerat och dessutom snabbt föränderligt vilket gör det svårt att beskriva hela området och dess sårbarhet. De operatörer som har intervjuats har varit mycket tillmötesgående, men det skall ändå påpekas att de är aktörer på en kommersiell marknad och att det kan finnas ekonomiska och konkurrensmässiga skäl till att ge en viss bild av verksamheten i samband med de intervjuer som genomförts.

Under arbetet har vi försökt att ta hänsyn till detta och ändå ge en så balanserad bild av systemen och dess sårbarheter som varit möjligt.

[2] Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap, avsnitt 4.2

[3] PTS diarienummer 02-12281

# 2 Hot mot elektronisk kommunikation

## 2.1 Klassificering av hoten

Analysen skall avse de båda situationerna svåra påfrestningar på samhället i fred resp. höjd beredskap och krig. Vid höjd beredskap bedrivs verksamhet för att förbereda Sverige för krig[4]. Begreppet svåra påfrestningar på samhället i fred har utvecklats under de senaste åren och beskrivs våren 2002 i propositionen om samhällets säkerhet och beredskap[5] på följande sätt:

> ”Regeringen angav i skrivelsen Beredskapen mot svåra påfrestningar på samhället i fred (skr. 1998/99:33) att en svår påfrestning inte är en enskild händelse i sig, exempelvis en olycka, ett sabotage osv., utan ett tillstånd som kan uppstå när en eller flera händelser utvecklar sig eller eskalerar till att omfatta flera delar av samhället. Svåra påfrestningar kan sägas utgöra olika slag av extrema situationer med låg sannolikhet som skiljer sig åt i sak. Tillståndet är av en sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen och därmed begränsa konsekvenserna.
>
> Det är emellertid inte möjligt eller ens önskvärt att, i generella termer, dra en skarp gräns mellan vad som är en händelse som kan innebära att en svår påfrestning på samhället i fred och vad som inte är det. Eftersom samhället skall ha en beredskap och förmåga att hantera alla typer av händelser i fred är det inte heller nödvändigt att definiera begreppet.”

Tänkbara hot som kan leda till eller uppträder vid svåra påfrestningar i fred kan delas in i sådana som slumpmässigt råkar drabba elektronisk kommunikation genom t.ex. oväder, naturkatastrofer eller olyckshändelser och sådana som har sitt ursprung i en aktör som avsiktligt söker påverka kommunikationen.

Tänkbara hot mot elektronisk kommunikation vid höjd beredskap och i krig har det gemensamt att de direkt eller indirekt är relaterade till den aktör som hotar landets frihet och självständighet eller utsätter landet för angrepp. De karakteriseras därmed i grunden av avsikten att skada. Även i detta fall är det svårt att dra en skarp gräns mellan hot vid svåra påfrestningar i fred och hot vid höjd beredskap och krig. Samma konkreta hot mot elektronisk kommunikation kan i fred komma från en politisk extremist och terrorist och vid höjd beredskap och krig från en sabotör från en angripande stat.

För att värdera rimligheten av och risken för olika typer av hot mot elektronisk kommunikation spelar det en betydande roll om hotet är avsiktligt eller inte. För att allvarliga störningar skall uppstå fordras ofta att flera funktioner, delsystem eller fysiska anläggningar drabbas samtidigt. Sannolikheten att slumpmässiga, oavsiktliga och oberoende hot skall inträffa samtidigt blir låg även om det finns en viss risk för att varje hot för sig skall inträffa. Däremot kan hot med ett och samma ursprung, t.ex. ett oväder, ungefär samtidigt beröra flera delar av ett kommunikationssystem. Den avsiktlige aktören däremot kan alltid förväntas söka agera så att samtidiga insatser mot olika mål förstärker varandra.

Ett utmärkande drag hos hot mot elektronisk kommunikation är att de ofta har en internationell dimension. Den yttrar sig dels genom att den elektroniska kommunikationen

[4] Lag (1992:1403) om totalförsvar och höjd beredskap

[5] Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap, sida 25

ingår i ett internationellt nätverk där Sverige är beroende av andra och där andra är beroende av hur nätverket och informationsöverföringen hanteras i Sverige. Den yttrar sig också genom att hot mot elektronisk kommunikation kan utövas över stora avstånd och med informationstekniska medel.

Informationsoperationer och informationskrigföring har blivit en väsentlig del av dagens konflikter. De moderna samhällenas allt mer omfattande spridning och utnyttjande av information i kombination med informationsteknikens snabba utveckling har gjort att information och informationssystem framstår som både ett tacksamt medel och åtråvärt mål för angrepp.

Tänkbara hot mot telekommunikationerna har tidigare analyserats i flera utredningar. En sammanställning av sådana analyser finns i en FOA-rapport från 1999[6].

## 2.2 Framtida konflikter

Avsiktliga hot mot elektronisk kommunikation måste bedömas mot bakgrund av en bredare bild av vilka konflikter som kan komma att beröra Sverige. Regeringen gör i propositionen om samhällets säkerhet och beredskap en sammanfattning av hotbilden för samhället sådan den bedömdes hösten 2001 i propositionen om totalförsvaret[7]:

> ”Regeringen ger i propositionen Fortsatt förnyelse av totalförsvaret sin syn på framtida konflikters karaktär. Bland annat betonas att samhället och befolkningen utgör både arena och mål för dagens våldsamma konflikter. Detta gäller oavsett om det är fråga om krigföring i mer traditionell mening, sofistikerade intrång i datasystem för att påverka ledningssystem, finansiella system, elförsörjning eller rena terroristhandlingar. Det finns anledning frukta att så kommer att vara fallet även i framtiden, såväl internationellt som om vårt land skulle drabbas. Totalförsvaret skall även ha förmåga att kunna anpassas för att, i ett förändrat omvärldsläge, kunna möta nya hot på kort, medellång och lång sikt.
>
> Det är enligt regeringen viktigt att både det militära och civila försvaret förbereds för såväl strid i bebyggelse och dess konsekvenser som att ickekonventionella medel kommer till användning. Även våldsangrepp från ickestatliga aktörer i denna miljö kan leda till stora konsekvenser i form av döda, skadade och förstörd egendom. Regeringen anser därför att det finns särskild anledning att belysa samhällets utsatthet i denna proposition.
>
> Regeringen har tidigare i propositionen Fortsatt förnyelse av totalförsvaret uttalat att vi inte kan utesluta att begränsade angrepp, med olika påverkansmedel, riktas mot Sverige i samband med en kris som utvecklas ur nuvarande omvärldsläge. Syftet kan vara att störa det svenska samhällets funktion eller att påverka vårt agerande. Det kan inte uteslutas att beslutsfattare påverkas av hot om våld mot befolkningen, särskilt med nukleära, biologiska eller kemiska stridsmedel.
>
> Teknisk infrastruktur, t.ex. elförsörjning och telekommunikationer, spelar enligt propositionen en allt viktigare roll för att kunna upprätthålla samhällets vitala funktioner. Sårbarheten i dessa system och den informationstekniska

[6] Sårbarhet i de civila telekommunikationerna av Ulf Pettersson, Petter Wulff, Georg Fischer, Försvarets forskningsanstalt (Numera Totalförsvarets forskningsinstitut) FOA-R--99-01221-240--SE oktober 1999 ISSN 1104-9154

[7] Regeringens proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret

utvecklingen har inneburit att även mindre intressegrupper, ekonomiskt svagare stater, terrorister och kriminella grupper fått större möjligheter att påverka, oavsett var i världen de befinner sig. Detta förhållande innebär att motståndsförmågan blir alltmer beroende av samhällsutvecklingen och ökar risken för att även en angripare med stora militära resurser väljer att i första hand rikta sina angrepp mot den civila infrastrukturen.

I propositionen pekar regeringen på att krig och fred under det kalla kriget har behandlats som två tydligt urskiljbara förhållanden. Idag riskerar vi istället att hamna i en situation där händelser, som var för sig inte nödvändigtvis går att betrakta som krigshandlingar, utvecklas utmed en glidande skala. I ett sådant läge skapas en gråzon mellan krig och fred där osäkerheten kommer att vara stor. Är vi utsatta för ett angrepp? På vilket sätt och i så fall av vem eller vilka? Är det fråga om en stat eller en ickestatlig aktör?

Regeringen framhåller vidare i propositionen att samhället måste kunna stå emot ett angrepp utfört av ickestatliga aktörer, som använder avancerade metoder och vapen likaväl som konventionella militära angrepp eller icke konventionella attacker från stater samt olika kombinationer av dessa. Risken för användning av B- och C-stridsmedel måste i ökande utsträckning uppmärksammas. Massförstörelsevapen kan te sig attraktiva också för terroristgrupper eller kriminella genom möjligheten att drabba många individer vid en attack eller en önskan att utföra mer spektakulära attacker. Ett hot om insats kan vara nog för att uppnå önskad effekt och det är svårare att skydda sig mot sådana attacker än mot traditionella attacker.

Befolkningens uppfattning om olika former av hot kan enligt propositionen bli avgörande för hur den klarar att hantera dem. Detta ställer krav på korrekt, saklig och snabb information. Osäkerheter om det inträffade eller oförmåga att på ett trovärdigt sätt förmedla information om det skedda kan inverka menligt på befolkningens förtroende och bidra till att förvärra effekterna av händelseutvecklingen.

Regeringen anser enligt propositionen att detta sammantaget innebär att samhällets robusthet, vår förmåga att hantera olika former av kriser, nationellt och internationellt, samt en grundläggande försvarsförmåga utgör viktiga delar av säkerhetspolitiken.”

## *2.3 Typer av påverkan*

I det följande redovisas en lista över några bedömt representativa hot indelade i slumpmässiga hot och avsiktliga hot. Hoten beskrivs primärt med hänsyn till hur systemen för elektronisk kommunikation påverkas med kommentarer till rimlighet i olika situationer i samhället i stort.

### 2.3.1 Slumpmässiga hot

#### 2.3.1.1 Extrema vädersituationer

Det kanske vanligaste hotet mot telekommunikationerna på grund av extremt väder riktar sig mot luftledningar som drabbas av avbrott på grund av snö och is i stora mängder. Denna typ av störningar inträffar så gott som varje vinter i någon eller några regioner i landet. Även svåra stormar utan snö och is men med många fällda träd kan ge liknande effekter. Också åska och blixtnedslag kan genom kopparledningar medföra omfattande

skador. I regel drabbas utrustning hos enskilda abonnenter men också utrustning i nätet kan skadas. Ofta drabbas samtidigt ett flertal såväl el- som teleledningar av störningar orsakade av väder. Det är framför allt glesbygd som drabbas.

Genom det ömsesidiga beroende som finns mellan el- och telesystemen försvåras situationen. Elavbrott gör att störningar kan uppstå också i nätelement och i stamnätet för elektronisk kommunikation och att basstationer i mobiltelefonnätet kan slås ut. Utslagna kommunikationer försvårar i sin tur insatser för att reparera skador och undsätta utsatta personer och verksamheter.

Störningar av detta slag är så pass vanliga att de som löper risk att drabbas ofta har viss beredskap för att hantera situationen eller har avstått från att göra sig beroende av t.ex. ständig datauppkoppling. Ofta finns batterireserver och reservkraft hos såväl el- och teleleverantörer som för vitala funktioner hos abonnenter. Reservsystemens uthållighet kan dock vara begränsad och kräva operatörsingripanden som kan vara svåra att genomföra. Skydd mot överspänningar ger visst skydd mot blixt men är inte alltid tillräckligt för att undvika skador.

Hotet mot telekommunikationerna från extremt väder kan begränsas genom förbättring av telenätet genom t.ex. bättre röjning av ledningsgator och ersättning av luftledning med nedgrävd kabel. Detta kan dock vara ganska dyrbart med få abonnenter att fördela kostnaden på. Med enbart kommersiella drivkrafter kan man därför befara att de flesta brister kommer att kvarstå under lång tid.

Något mindre vanligt än snö och is men ändå förekommande är avbrott och störningar i samband med stora översvämningar. Kablar kan då förstöras när vägbankar eroderas eller broar förstörs och elektronisk apparatur kan sättas ur funktion av vatten och fukt. Det är då inte nödvändigtvis bara utpräglad glesbygd som drabbas utan även tätorter**.** Ett exempel på detta utgjorde ovädren och översvämningarna på Orust sommaren 2002 när även telekommunikationerna delvis slogs ut med konsekvenser för bl.a. räddningsinsatserna.

Hur mycket leveranssäkerheten än förbättras kommer det inom överskådlig tid alltid att finnas kvar en risk att elförsörjning och de elektroniska kommunikationssystemen slås ut av extremt väder. I extrema fall kan då konsekvenserna bli så stora att omfattande extraordinära insatser från flera samhällsfunktioner måste göras för att lindra verkningar och hantera situationen. Regionala störningar eller avbrott i el- och teleinfrastrukturen i samband med extremt väder leder ofta till och förekommer samtidigt som en mängd störningar och problem inom ett stort antal områden i samhället. En väl fungerande och förberedd ledning och tillgång till mobila reservsystem är då av stor betydelse. Erfarenheter från t.ex. den svåra isstormen i östra Kanada år 1998 illustrerar detta. (Jämför avsnitt 4.2.1).

#### 2.3.1.2 Tekniska fel, felaktig hantering och olyckor

Trots alla satsningar på säkerhet under normala förhållanden hindrar det inte att slumpmässiga fel ändå kan uppstå som får stora konsekvenser. Det kan bero på t.ex. tekniska fel i hård eller mjukvara, felaktig hantering vid driften av systemen eller yttre olyckor av olika slag som drabbar också systemen för elektronisk kommunikation.

En vanligt förekommande felorsak är att kablar grävs av eller på annat sätt skadas. Oftast är det möjligt att i centralare delar av näten göra omkopplingar och välja andra vägar så att avbrotten i kommunikationerna blir mycket begränsade. Om emellertid ytterligare avbrott skulle inträffa nära i tiden så att även de alternativa vägarna i nätet blockeras kan konsekvenserna bli större. Så var till exempel fallet när teletrafiken till och från Norrland bröts i oktober 2001. En avbruten lokal förbindelse som betjänar viktiga funktioner i

samhället kan också medföra svåra påfrestningar. Riskerna kan i sådana fall minskas genom att viktiga funktioner skaffar sig flera oberoende kommunikationsmöjligheter.

Andra fel som kan få stora konsekvenser om inte redundans och reserver är tillräckliga är tekniska fel i nätens elektroniska apparatur och i mjukvara. Särskilt stora är riskerna för fel i samband med utbyte eller uppgradering av utrustning och mjukvara.

Elektronisk kommunikation hotas också av bränder, explosioner och ras som berör tunnlar och lokaler där kablar dragits eller där nätutrustning av olika slag placerats.

Elberoendet är stort. Batterier och reservkraft kan i regel klara elbortfall under några timmar, men långvariga avbrott som berör många nätelement kan vara svåra att hantera. Även om operatörernas reservsystem fungerar vid elavbrott är risken stor att många abonnenter saknar reservkapacitet vid sina egna anläggningar. Det gamla fasta telefonnätet har elförsörjning ut till abonnenten i själva telenätet men alla andra typer av elektronisk kommunikation, digitaliserad liksom mobil, kräver egen elförsörjning hos abonnenten. Mobiltelefoner har dock relativt lång drifttid på egna batterier och kan lätt laddas också via billaddare.

I samband med en svår påfrestning på samhället av något annat skäl t.ex. en större olycka kan belastningen på systemen för elektronisk kommunikation bli långt större än normalt med utslagning på grund av överbelastning som följd.

I perifera delar av nätet kan tekniska fel, felaktig hantering och olyckor lätt leda till bortfall av telekommunikationerna. Här finns i regel endast en förbindelse, en server etc. och därmed ingen reservmöjlighet eller alternativ kopplingsväg. Å andra sidan blir verkningarna av ett avbrott endast lokala och därmed är i regel sannolikheten liten att ett avbrott skulle leda till svåra påfrestningar på samhället. För samhällsviktiga verksamheter kan dock konsekvenserna av ett avbrott bli stora. För sådana är det därför angeläget att söka skapa redundans och extra hög tillgänglighet också på den lokala nivån.

Längre in i näten förekommer naturligtvis tekniska fel, felaktig hantering och olyckor men konsekvenserna kan i regel begränsas genom att man utnyttjar reserver och omkopplingsmöjligheter. Ett problem kan vid mer avancerade fel vara att ha tillgång till tillräckligt kompetent personal i erforderlig omfattning. För att konsekvenser av fel skall bli små är det viktigt såväl att minska risken för att fel uppstår som att ha en god förmåga att hantera dem när de trots allt uppkommer. För relativt ofta förekommande typer av fel blir det för operatörerna en avvägningsfråga hur mycket man skall satsa på säker teknik, redundans, experter och reserver i förhållande till kostnaderna för att ha avbrott i tillgängligheten. Dagens IT-samhälle ställer höga krav på tillgänglighet av elektroniska kommunikationer och förmågan att tillgodose kraven blir ett konkurrensmedel för operatörerna. På en marknad med ett flertal operatörer finns därför incitament att utforma systemen så att funktionssäkerheten blir hög i de mer centrala delar som många abonnenter är beroende av. När det gäller olika former av inre störningar som uppstår inom de egna systemen har operatörerna också goda möjligheter att med tillräckliga satsningar uppnå en mycket hög säkerhet.

I de perifera delarna av nätet är det däremot i regel inte ekonomiskt eller marknadsmässigt försvarbart att ha sådan säkerhet att enstaka fel inte påverkar kommunikationen. Där blir det i stället viktigt att de trots allt sällan förekommande felen snabbt kan repareras.

Även i nät med redundans i form av signalmässigt åtskilda vägar kan fysisk påverkan få påtagliga konsekvenser om inte de elektroniskt skilda vägarna också är rumsligt åtskilda. Ofta dras av praktiska skäl och kostnadsskäl många olika kablar i samma kabeltrummor och förläggs tillsammans med annan viktig infrastruktur. Strävan brukar dock vara att inte samlokalisera centrala funktioner i oberoende system. Ibland sker dock detta i vad man

bedömer vara väl skyddade utrymmen, något som kan ge stora konsekvenser om skador trots allt uppkommer i sådana utrymmen.

De elektroniska kommunikationerna särskilt till de norra delarna av landet och till Gotland är beroende av ett fåtal stamledningar. Tillkomsten av fler operatörer har dock gjort att redundansen totalt sett förbättrats. Intervjuer med operatörer har indikerat att samverkan mellan olika operatörer vid svårare störningar ännu är så pass outvecklad att den principiellt befintliga redundansen torde vara svår att utnyttja i praktiken.

### 2.3.2 Avsiktliga hot

De avsiktliga hoten mot elektronisk kommunikation kännetecknas av att de skapas av en aktör som med sitt agerande har något syfte som i regel är vidare än att påverka telekommunikationerna i sig. Det kan handla om allt från att pojkstrecksaktigt demonstrera sin egen förmåga att nästla sig in i ett system till att i väsentliga avseenden förhindra samhällets funktion. Beroende på syftet och den situation i stort där ett hot uppträder ter sig olika medel för att realisera det mer eller mindre rimliga och möjliga.

Regeringen bedömer som påpekats ovan att risken ökar att såväl angripare med stora militära resurser som resurssvagare aktörer som vill skada samhället väljer att angripa den tekniska infrastrukturen. Möjligheterna att påverka systemen, sårbarheten och de tänkbart stora konsekvenserna gör infrastrukturen till ett lockande mål.

Angrepp mot elektronisk kommunikation kan ske med fysiska medel alltifrån enklare skadegörelse och sabotage till angrepp med militära medel. Angrepp kan också ske med informationstekniska medel utan att någon direkt fysisk åverkan sker. Telekommunikationerna kan också skadas av angrepp som primärt riktas mot andra mål men där verkningarna även berör elektronisk kommunikation. Mest påtagligt gäller detta elförsörjningen.

För att de avsiktliga hoten mot elektronisk kommunikation skall bli verkningsfulla krävs i regel en viss kännedom om kommunikationssystemens uppbyggnad och funktion. Generell kunskap går att få då näten vanligen innehåller komponenter från ett fåtal stora leverantörer och att kunskapen är relativt spridd om hur utrustningar och nät fungerar. Möjligheterna att skada systemen blir dock mycket större för den som har tillträde till anläggningar och behörighet att hantera driften, koppla upp sig på styrsystem etc. Detta gör att hot från så kallade insiders måste tas på särskilt allvar. Enstaka individer med onda avsikter bland alla anställda, konsulter, entreprenörer och leverantörer som är inblandade i uppbyggnad och drift av kommunikationssystemen skulle med rätt kompetens och behörighet kunna åstadkomma stor skada.

Svåra påfrestningar kan uppstå vid angrepp som berör elektronisk kommunikation som har stor betydelse för nyckelfunktioner i samhället. Exempel på sådana funktioner utgörs av SOS alarmering, sambandscentraler för polis och räddningstjänst, ledningsorgan för samhällsviktig verksamhet särskilt krisledning, noder och stammar i kommunikationsnätverk, system för att sprida massmedial information, styr- och ledningscentraler för transportsystem etc. Sådana funktioner skulle kunna angripas av den som vill påverka samhällsfunktionen i stort. Det kan handla om en militant aktivist som vill angripa t.ex. multinationella företag. Det kan handla om en terrorist som vill skapa rädsla och minska befolkningens tilltro till samhällets funktion. Det kan handla om en sabotör som vill minska vår försvarsförmåga inför ett militärt angrepp mot mål i Sverige. Eller det kan handla om ett militärt angrepp genom luften för att slå ut infrastruktur och därigenom söka påverka Sveriges agerande. En aktör av detta slag är sannolikt mindre

intresserad av just telekommunikationerna utan vill påverka dem som använder sig av dessa. Därför kan ett angrepp tänkas ske kombinerat mot flera typer av mål.

#### 2.3.2.1 Fysisk påverkan

En mycket stor del av de elektroniska kommunikationerna förmedlas genom ledningar, kablar och apparatur som i regel saknar fysiskt skydd och är lätt tillgängliga för åverkan. Det går att med enkla medel klippa av ledningar och kablar och att förstöra utrustning så att kommunikationerna lokalt slås ut. Insatser av detta slag ter sig rimliga främst från en aktör som vill skada någon individ, en organisation eller ett företag eller vill sabotera en viss verksamhet. Det kan också handla om att förhindra larm eller tillkallande av hjälp i samband med inbrott eller annan brottslig verksamhet. Normalt medför detta inte någon svår påfrestning för samhället såvida det inte handlar om en nyckelfunktion där. Några insatser för att öka skyddet mot enklare fysisk åverkan på systemen för elektronisk kommunikation ter sig därför i allmänhet knappast mer befogade än sådant inbrottsskydd och polisiärt skydd som finns i stort.

Enklare påverkan genom avklippta kablar eller sönderslagen utrustning kan få större påverkan på den elektroniska kommunikationen om skadegörelsen sker på platser med stor koncentration av kablar till samma fysiska område för elektroniskt åtskilda kommunikationssystem eller vid samtidig påverkan på flera ställen så att nätverkens redundans urholkas. En viktig förutsättning för att nå stor verkan är kännedom om nätens uppbyggnad och var särskilt känsliga punkter för påverkan finns. Det torde vara svårt att utan ”insider”-information på ett effektivt sätt genom fysisk åverkan på ett avgörande sätt sabotera systemen för elektronisk kommunikation. Ett undantag kan möjligen vara mobiltelefonsystemen och radiolänkförbindelser där det torde vara relativt lätt att kartlägga var antenner och master är lokaliserade. En insats för att förstöra många sådana mål blir å andra sidan omfattande och resurskrävande.

Ett exempel på hur relativt enkla men samtidiga ingrepp på flera platser ändå kan drabba vitala funktioner utgörs av det sabotage mot ett antal kommunikationskablar i Madrid som gjordes i juni 2002. Det fick följder för samhällsviktiga funktioner, bland annat drabbades fyra flygplatser av stora förseningar.

För att påverka bättre skyddade anläggningar krävs mer avancerade metoder såsom sprängning eller angrepp med tyngre vapen samt, för att nå god effekt, kunskap om systemuppbyggnad och vad som utgör känsliga punkter.

Enligt aktuella hotbedömningar ter sig militära angrepp syftande till invasion av Sverige för lång tid inte rimliga. Däremot kan andra mer begränsade militära angrepp mot mål i Sverige inte helt uteslutas även om de ter sig mycket osannolika. De skulle kunna riktas mot infrastrukturen och kan främst tänkas ske genom luften med robotar eller flyg eller genom sabotage eller rädföretag. Möjlig precision vid angrepp genom luften har genom den militärtekniska utvecklingen blivit mycket hög. Även här fordras stor systemkunskap för att kunna nå hög verkan. Angrepp mot elförsörjningen, som kan vara lättare att kartlägga och angripa, kan dock få stor effekt också på systemen för elektronisk kommunikation.

En speciell typ av hot mot elektroniska system utgörs av mycket starka elektromagnetiska fält. Sådana kan genereras momentant genom en stark urladdning och därvid uppstående elektromagnetisk puls. Det är möjligt att konstruera elektromagnetiska vapen som kan ha stor verkan mot elektronisk utrustning som inte är skärmad mot det elektromagnetiska fältet**.** Redan för att få verkansavstånd av storleksordningen några hundra meter krävs dock relativt stora och plattformsburna system. En terrorist med ett tänkbart handburet system

skulle knappast kunna uppnå någon permanent skada mer än i sin omedelbara närhet eller kunna orsaka störningar på avstånd större än ca 50 meter.[8]

#### 2.3.2.2 IT-relaterade hot

Intrång i och manipulation av informationssystem (informationskrigföring) är ett hot som växer i takt med att det svenska samhällets beroende av informationssystem ökar. Det hot som för närvarande bedöms som det allvarligaste i det sammanhanget är intrång i datasystem av olika slag via teleförbindelser eller Internet för att manipulera dem och störa till exempel elförsörjning, telesystem och betalningar.

Något som på allvar skulle äventyra upprätthållandet av samhällets funktion vore en väl planerad massiv intrångsattack mot vitala stödsystem för samhällsviktiga funktioner. En sådan skulle allvarligt kunna störa exempelvis elförsörjning och elektronisk kommunikation. Telekommunikationerna skulle kunna utsättas för direkta intrång i systemdriftsdatanäten där någon sedan har möjlighet att koppla bort olika system. Indirekt påverkan genom illasinnad kod, exempelvis virus, trojanska hästar eller maskar är ett annat tänkbart hot.

För en sabotör är intrång och angrepp via Internet attraktivt då det är möjligt att verka på stora avstånd utan fysisk närvaro. Det är dessutom ofta svårt att spåra varifrån angreppet kommer vilket medger en hög grad av anonymitet. Ett misslyckat angreppsförsök kan relativt lätt förnyas eller riktas mot andra punkter i systemen utan att risken för avslöjande markant ökas. De resurser som krävs i form av dyrbar utrustning för ett IT-angrepp är idag relativt sett små, isynnerhet i jämförelse med kostnaden för de system som angrips. IT-hoten är på ett helt annat sätt än andra hot mot elektronisk kommunikation internationella, närmast globala till sin karaktär.

En stor svårighet för den anonyme aktören som agerar på distans är att ha tillräcklig kunskap om de system han söker störa eller göra intrång i för att kunna agera med precision. Insiderkunskap utgör därför en stor och i många fall nödvändig tillgång för den som vill störa eller göra intrång i telenätens styrsystem. Insidern kan exempelvis vara en anställd, konsult eller underleverantör som har eller lätt kan skaffa sig nödvändig behörighet till systemen.

Ett annat vanligt IT-hot är så kallade överbelastningsattacker där man slår ut en server genom att låta ett stort antal klienter anropa servern samtidigt. Servern hinner då inte med att besvara alla anrop. Dessa så kallade DDoS-attacker (Distributed Denial of Service) har ännu så länge varit vanligast på Internet. Det är dock inte otroligt att de mobila telenäten kommer att drabbas i framtiden med framväxandet av ett mobilt Internet. En basstation eller växel skulle då kunna blockeras av att tusentals mobilterminaler samtidigt förmås att försöka ringa. Detta skulle kunna ske genom spridning av illasinnad kod till mobiltelefoner.

Dagens elektroniska system är uppbyggda av en mängd komponenter i form av integrerade kretsar som samlas ihop på kretskort. Många av dessa kretskort är programmerbara och har kod som används i specifika tillämpningar inom exempelvis elektronisk kommunikation. Kretskort kan även innehålla dold kod som inte är känd av andra än tillverkaren. Detta kan vara kod som finns där i syfte att underlätta test av kortet. Men en mindre seriös tillverkare, eller en insider hos tillverkaren, skulle även kunna lägga in kod med andra syften. Kretskort finns även i exempelvis basstationer där den som vill skada eller utnyttja systemet relativt lätt skulle ha möjligt att byta ut eller manipulera med kretskorten. Ett

[8] Elektromagnetiska vapen och skydd, FOI orienterar om nummer 1 2001, Totalförsvarets forskningsinstitut

syfte skulle då till exempel kunna vara att på en bestämd signal stänga av radiobasstationen.

Hotbilden med avseende på IT förändras hela tiden. När en säkerhetslucka har upptäckts kommer det vanligen snabbt lösningar och uppgraderingar som stänger luckan. Andra systemuppgraderingar som syftar till exempelvis ökat tjänsteutbud kan samtidigt öppna nya hål i säkerheten. Angriparna å sin sida utvecklar hela tiden nya angreppsmetoder och letar efter brister i de olika säkerhetssystemen. Mängden potentiella angripare ökar dessutom hela tiden då antalet användare med kunskap om IT ökar i världen.

Militärt förekommer en mångfacetterad verksamhet av informationstekniskt slag som med ett samlingsnamn brukar kallas telekrigföring. Sådan går bl.a. ut på att avlyssna en motståndares radiokommunikation, störa hans sambandssystem, spaningsorgan och målsökare, skydda eget samband, kamouflera egna system samt att sprida vilseledande information. Telekrigföring kan förväntas ingå som en del av militära angrepp mot den tekniska infrastrukturen i samhället om sådana angrepp skulle aktualiseras. Mycket av de militära metoderna kan äga tillämpning också vid fredstida aktioner mot civila system för elektronisk kommunikation. Det kan t.ex. gälla störning av radioförbindelser eller intrång i, avlyssning av och falsk signalering i kommunikationsnätverk.

#### 2.3.2.3 Icke-konventionella stridsmedel

Elektroniksystem och ledningar är särskilt känsliga för den elektromagnetiska puls, EMP, som uppstår vid kärnvapenexplosioner. En sådan explosion på hög höjd skulle genom den elektromagnetiska pulsen kunna få verkan på avstånd som vida överstiger andra verkansformer, i princip inom det område som ligger ovanför horisonten. Det har spekulerats i om detta skulle kunna utgöra en speciell form av kärnvapenkrig. Idag betraktas dock knappast ett isolerat hot från höghöjds-EMP som särskilt rimligt, dels för att det ändå skulle innebära en upptrappning till kärnvapennivå, dels för att dess verkan vore mycket tveeggad.

Biologiska och kemiska stridsmedel ter sig som något mer påtagliga risker t.ex. utnyttjade av terrorister eller vid konflikter som inkluderar regimer i så kallade skurkstater. B- och C-stridsmedel riktar sig inte mot systemen för elektronisk kommunikation i sig men skulle om de kom till användning skapa en utpräglad krissituation med stort behov av bl.a. väl fungerande telekommunikationer. Det finns därför skäl att inom ramen för de skyddsåtgärder som vidtas för att kunna hantera en situation med ett B- eller C-angrepp också beakta behovet av skydd för personal som kan upprätthålla telekommunikationerna.

# 3 Systemen och deras sårbarheter

I det följande beskrivs systemen för elektronisk kommunikation och deras sårbarheter. De tre första avsnitten behandlar telenät, först telenät i allmänhet, därefter beskrivs det fasta telenätet följt av olika mobila telefonisystem. Det fjärde avsnittet ägnas åt data-kommunikation med en viss fokusering på IP-telefoni och Internet.

Dessa system har olika grader av likheter och skillnader. Gemensamma egenskaper är beroendet av en nätinfrastruktur med hög överföringskapacitet samt beroendet av el. Betydelsen av detta diskuteras i avsnitten 3.5 och 3.6. Slutligen diskuteras utvecklingen av systemen i framtiden och vilken påverkan detta kan ha på sårbarheten.

## *3.1 Funktionerna i ett telenät*

Telefonnäten bygger traditionellt på kretskopplad teknik. Det innebär att en förbindelse kopplas mellan två abonnenter. Denna förbindelse är uppkopplad under hela samtalet med reserverad bandbredd oavsett om abonnenterna talar med varandra eller inte.

Dagens telefonnät är heller inte enbart anpassade för tal utan används även i stor utsträckning för att överföra data. I den följande översiktliga beskrivningen görs ingen skillnad mellan trafik i form av tal eller data.

För att använda ett telefonnät måste man ha tillgång till en telefon eller terminal som i sin tur står i förbindelse med telefonnätets accessnät. Är detta uppfyllt för en abonnent kan denne utnyttja telefonnätet för att ringa upp en annan abonnent. Genom att de flesta telefonnäten idag är sammanbyggda behöver de två abonnenterna idag inte befinna sig i samma nät. De kan använda sig av olika typer av nät drivna av olika operatörer i skilda länder.

### 3.1.1 Accessnät

Accessnätet har till uppgift att samla ihop trafiken från abonnenterna och koncentrera denna på så få förbindelser som möjligt. Accessnätet sträcker sig från abonnenten till närmaste telestation. För fast telefoni, den äldsta formen av telenät, utgörs accessnätet huvudsakligen av koppartrådar. Många myndigheter och företag har idag optisk fiber ända fram till sina lokaler, för privata abonnenter är detta fortfarande relativt ovanligt. För mobiltelefoni utgörs accessnätet av en radioförbindelse mellan telefonen och en basstation.

### 3.1.2 Transportnät

Efter accessnätet följer transportnätet vars uppgift är att överbrygga avstånd och knyta samman de olika telefonstationerna i nätet. Detta nät utgörs till stor del av optiska fibrer men även radiolänk. Man brukar till detta nät även räkna in den utrustning som behövs för att förstärka, sammanfoga och koppla om signaler.

### 3.1.3 Nätelement och nätintelligens

Telefonstationerna innehåller bland annat växlar. Växlarna analyserar det nummer som abonnenten slagit och ser till att samtalet kopplas rätt. För detta kan det krävas slagningar i abonnentdatabaser. Det är även i växeln som samtalet debiteras abonnenten.

Det finns även speciella noder som tillhandahåller speciella tjänster. Dessa noder programmeras enligt en fastställd standard, IN (Intelligent Network). Detta gör att man snabbt kan ändra och införa nya IN-tjänster i ett nät genom att byta ut programvaran i dessa noder.

IN-noderna kan programmeras till att styra om samtal till olika platser beroende tid på dygnet eller varifrån samtalet kommer. Andra exempel på IN-tjänster är frisamtal, betal-samtal, personligt nummer och virtuella privata nät.

För att koppla upp och ner samtal och tillhandahålla olika typer av tjänster krävs det även datatrafik i näten. Denna trafik behöver inte gå samma väg genom systemet som själva samtalen. I moderna telenät finns ett speciellt signaleringsnät som fungerar som ett datanät mellan stationerna.

### 3.1.4 Näthantering

För att driva ett telenät så behövs drift och underhåll, ofta kallat näthantering (Network Management). Drift innebär hantering av abonnenter, att lägga till, ändra och avsluta abonnemang, taxering, det vill säga att ta betalt av abonnenterna. Det innebär även trafikoptimering för att maximera nyttjandegraden och undvika överbelastning. Att lägga till, ta bort och uppgradera tjänster i nätet är även det en del av driftverksamheten. Underhåll innebär mätning och övervakning av nätet samt felsökning och avhjälpande av fel.

Ett effektivt drift- och underhållsarbete förutsätter att operatören kan kommunicera med telesystemet. Systemet ska bland annat kunna larma om fel, ge besked om utrustningars status och lämna driftstatistik. Man vill även kunna beordra mätningar, omdirigera trafik eller införa ändringar i systemen.

Tidigare var det mesta av arbetet manuellt, nu i större utsträckning fjärrstyrt och automatiserat. För att förenkla och förbilliga drift- och underhållssystemen finns standarder som beskriver gränssnitt mellan olika typer av utrustning och var en viss funktionalitet ska placeras.

### 3.1.5 Allmänt om sårbarhet i telenät

Ett fungerande telefonnät handlar traditionellt om obrutna förbindelser. Tal och data måste överföras mellan abonnenterna. Styrsignaler måste förmedlas mellan olika nätelement. Misslyckas man med detta kommer inte abonnenterna i kontakt med varandra.

För att upprätthålla en obruten förbindelse mellan två punkter i telefonnätet måste man se till att alla de nätelement, kablar och länkar som ingår i en förbindelse mellan dessa två punkter är oskadade. Att gardera sig mot oskadade kablar genom fysiskt skydd och övervakning skulle bli mycket svårt på grund av nätets storlek. När ett avbrott ändå inträffar kommer delar av nätet att vara onåbara till dess att förbindelsen är reparerad.

En lösning är att man medvetet konstruerar nätet med redundans. Redundans innebär att det finns alternativa förbindelser mellan punkterna. Det betyder att om en väg genom nätet bryts så kan man snabbt dirigera trafiken en annan väg och fortfarande ha kontakt. Samtidigt kan man påbörja reparation av den avbrutna förbindelsen.

Eftersom trafiken i telenät koncentreras till nätens centrala noder och till transportnätet drabbar skador i dessa delar fler abonnenter än skador i perifera nätelement och i accessnätet. Det är därför generellt sett viktigare med redundans i de centrala delarna.

Allt mer information förmedlas som datatrafik i dagens telenät. Dagens telenät har en mer komplex natur än tidigare, det är fler olika system som interagerar, dessutom är betydligt fler aktörer involverade. Det kan därför finnas en osäkerhet om den information som transporteras. Når informationen rätt mottagare? Kan mottagaren säkert identifiera avsändaren? Kan man verifiera att den information som kommit fram är densamma som skickades?

## 3.2 Fasta telenät

### 3.2.1 Nät

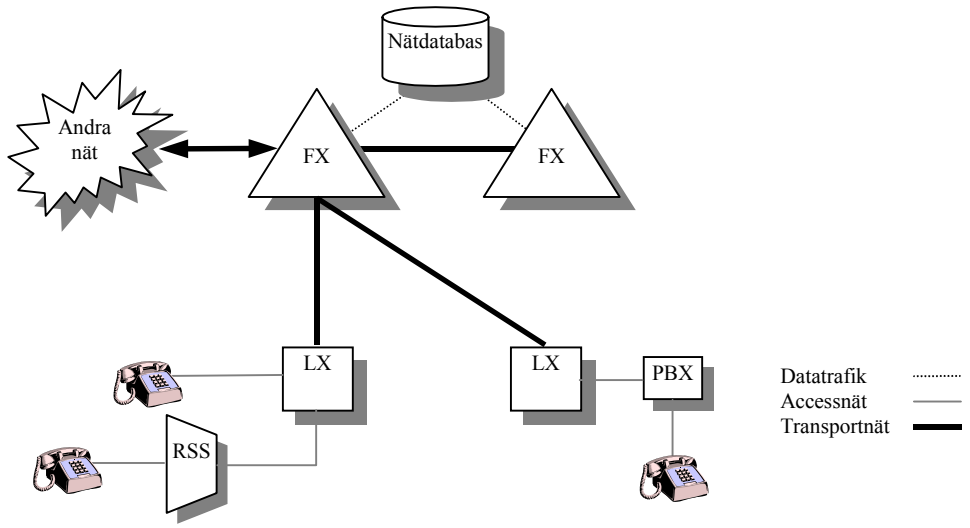
Tidigare byggde tekniken i de fasta telefonnäten helt på analog teknik och elektromekaniska växlar. Idag har man nästan helt övergått till digital teknik. Undantag finns huvudsakligen i accessnätet. Den vanligaste accessformen är fortfarande koppartråd till hushåll från närmaste station vilket normalt innebär analog förbindelse. Men digitala förbindelser (främst ISDN och ADSL) kan också erbjudas på koppartrådar. På vägen mellan hushåll och lokalstation finns kopplingspunkter där fler anslutningar samlas ihop. Många stora företagsväxlar är anslutna med optisk fiber.

Transportnätet utgörs huvudsakligen av optiska fibrer och till en viss del av radiolänk. Det fasta telenätet är optimerat för taltelefoni. Varje talkanal kräver, efter digitalisering i abonnentsteget, en överföringskapacitet på 64 kbit/s. Andra ändutrustningar som till exempel fax och modem måste anpassa sig till dessa talkanaler. Den lägsta nivån i transportnätet är 2 Mbit/s, vilket motsvarar 30 talkanaler plus två kanaler för signalering och synkronisering. I en optisk fiber kan man idag få in upp till 10Gbit/s. Det vill säga att en optisk fiber teoretiskt kan förmedla cirka 150 000 telefonsamtal.

### 3.2.2 Stationer och växlar

Bilden nedan visar den principiella strukturen för ett nät för fast telefoni.

Abonnenten ansluter sig via sin telefon till ett abonnentsteg vilket kan finnas i en lokalstation (LX – Local eXchange). Det finns även utbrutna abonnentsteg placerade separat från lokalstationen (RSS – Remote Subscriber Step). Företag och myndigheter kan ha egna växlar (PBX – Private Branch eXchange). Dessa integreras ofta med företagets interna datasystem, för att exempelvis få upp information från en databas då en känd kund ringer.




En intressant aspekt är att elförsörjningen av den enskilde abonnentens telefon sker via kopparledningen i accessnätet. Detta gör att abonnentens telefon fungerar så länge abonnentsteget är strömförsörjt, oavsett om abonnenten för övrigt har fungerade elförsörjning eller inte.

I lokalstationen (LX) kopplas och debiteras samtalen. Om abonnenterna tillhör samma lokalstation hanteras samtalet av denna. Den normala vägen för ett samtal mellan

abonnenter tillhörande olika lokalstationer är via förmedlingsstationerna (FX). Även andra typer av kopplingar och förbindelser kan förekomma.

Det är på FX-nivån som kontakter med andra nät finns. För att ringa en person i ett annat nät måste samtalet passera förmedlingsnivån.

Lokalstationer och accessnät ägs idag till största delen av Telia. Andra operatörer kan dock koppla in sig på lokalstationerna och hämta sina kunders trafik därifrån.

Vissa tjänster i det fasta telenätet kräver tillgång till en central nätdatabas.

### 3.2.3 Sårbarheten i det fasta telenätet

Utgående från det fasta telenätets olika delar och de hotbilder som diskuterats tidigare kommer vi i det följande att diskutera vilka effekter olika händelser kan få för det fasta telenätets funktion.

Accessnäten är sårbara. Accessnätet skall nå ända fram till abonnenten och finns därför där människor verkar och rör sig. Luftledningar finns fortfarande i stor utsträckning och dessa är exponerade för extremt väder. Men även nergrävda kablar drabbas ofta av avbrott. Accessnätet består till stor del av kopparledningar. Blixtnedslag och elektromagnetiska vapen kan därför ge överslag som förstör näten eller utrustning ansluten till den. Redundansen i accessnätet är låg och enstaka störningar får därför direkt effekt. Det är lätt för en sabotör att tillfoga accessnäten skador genom att exempelvis klippa av ledningar på olika ställen. Det bör dock framhållas att effekterna av skador i accessnätet är begränsade i utsträckning och att varje störning normalt endast berör ett mindre antal abonnenter. Men sabotörer skulle kunna isolera ett utvalt mål genom att angripa accessnätet.

Att från grunden bygga ett heltäckande accessnät för fast telefoni som alternativ till det idag existerande är inte intressant och framför allt för dyrt. För digital anslutning finns det idag i viss utsträckning alternativ i form av kabel-tv-nätet, elnätet och fiber ända fram till abonnenten. Tekniken för telefoni via elnäten är ännu inte riktigt mogen, framför allt då den orsakar radiostörningar. Fiber ända fram till abonnenten är kostsamt och utnyttjas idag till största delen av företag och myndigheter, men även i ökande utsträckning av privata abonnenter. Kabel-tv-nät är mer spridda. Digitala anslutningar används för datatrafik, men ger även ett alternativ till traditionell telefoni genom möjlighet till IP-telefoni (jämför avsnitt 3.4.2).

Det fasta telenätet är beroende av ett transportnät, en nätinfrastruktur med hög överföringskapacitet. I avsnitt 3.5.1 förs en diskussion om sårbarheten i IT-infrastruktur med hög överföringskapacitet. Denna diskussion är till stor del även applicerbar på transportnätet i det fasta telenätet.

Varje förbindelse i transportnätet förmedlar normalt en mycket större mängd trafik än en förbindelse i accessnätet. Skador i transportnätet kan därför ge större effekt i form av antal drabbade abonnenter. På denna nivå är det därför viktigare med en hög grad av redundans för att kunna koppla runt enstaka avbrott. På detta sätt uppnår man en minskad sårbarhet mot framför allt slumpmässiga hot. Det finns därför alltid minst en alternativ väg från lokalstation och uppåt så att enstaka kabelbrott inte skall påverka trafiken.

Nätelement som telestationer och växlar är känsliga punkter. Bortfall av ett abonnentsteg leder till att alla teleförbindelser inom abonnentstegets område försvinner, vilket drabbar ett hundratal upp till något eller några tusental abonnenter. Bortfall av en lokalstation innebär att tiotusentals abonnenter drabbas. De utbrutna abonnentstegen som hör till stationen går i detta fall över i autonom drift. Det innebär att man bara kan ringa enkla samtal till abonnenter kopplade till samma abonnentsteg. Normalt vet inte abonnenterna

om de är anslutna via ett utbrutet abonnentsteg eller direkt till ett abonnentsteg i en lokalstation. Vid bortfall av stationer på förmedlingsnivån tappar man möjlighet att kommunicera utanför det lokala området och eventuellt förmågan att kommunicera med andra telefonnät. Skulle detta inträffa drabbas hundratusentals abonnenter. Skador på nätelement kan vara svårare att felsöka och reparera jämfört med skador på förbindelser i nätet.

Om en lokalstation tappar förbindelsen till förmedlingsnivån kan man fortfarande ringa inom lokalstationens område och man har tillgång till de tjänster som finns i lokalstationen (exempelvis PLUS-tjänster), men tilläggstjänster som kräver nätdatabaser (IN) fungerar inte.

Eftersom skador på nätelement från lokalstation och uppåt ger stora effekter vid bortfall är det viktigt med skydd och redundans. Idag tillhandahåller PTS ett tjugotal bergrum i landet som skall ge ett gott skydd mot precisionsvapen och även mot elektromagnetiska vapen. Skanova[9] har även egna bergrum. En stor del av den viktiga utrustningen finns lokaliserad i dessa bergrum. Detta är både en styrka och en svaghet. Å ena sidan ger dessa bergrum ett mycket gott skydd. Å andra sidan kan en angripare som lyckas slå ut ett helt bergrum med innehåll tillfoga telenätet mycket stor skada. Detta drabbar inte enbart det fasta nätet utan skulle även drabba datatrafiken och de mobila näten då denna utrustning står i samma lokaler. Man har system för inpassering till bergrum men samtidigt är det många som har tillträde, personal från operatörer, entreprenörer, leverantörer och städpersonal. Utrustning från lokalstation och uppåt är dubblerad så det finns redundans.

Styrning och övervakning av trafiken sker från centrala punkter via systemdriftsdatanät. Detta innebär att man kan få en samlad bild av nätets tillstånd. Störningar kan snabbt upptäckas och hanteras. Detta reducerar sårbarheten vid slumpmässiga hot då man lättare kan styra om trafiken vid störningar. Men det innebär samtidigt en ökad sårbarhet för avsiktliga hot. En angripare som skaffar sig fullständig tillgång till datanätet skulle i princip kunna stänga ner hela nätet. Det är därför mycket viktigt att datanäten har kraftfulla skydd som förhindrar intrång och begränsar möjligheterna att nå stora delar eller hela nätet då någon eventuellt lyckas ta sig in.

För att komma åt systemdriftsdatanät i det fasta telenätet krävs vanligen att man har direkt tillgång till en terminal. Dessa terminaler finns inte allmänt tillgängliga så för att skaffa sig tillgång till dessa IT-system krävs först att man gör fysiskt intrång. Själva systemen skyddas sedan av intrångs- och behörighetssystem där olika användare har olika rättigheter så att det ska vara mycket svårt för någon att av misstag ställa till med stor skada. IDS (Intrusion Detection Systems) används för att varna om något onormalt inträffar, exempelvis om någon användare försöker utföra något den normalt inte brukar göra. Det hot som är svårast att skydda sig mot är att någon, exempelvis anställd eller konsult, med kunskaper och rättigheter i systemet medvetet går in för att skada systemen.

El är en ofrånkomlig förutsättning för att telekommunikationerna skall fungera. Avbrott i elförsörjningen får omedelbart effekt på de komponenter av telenätet som drabbas. Sårbarheten för detta är reducerad genom att all utrustning från lokalstationer och uppåt är utrustade med batterier och fasta reservkraftsaggregat. Utbrutna abonnentsteg har batterireserver på 4-8 timmar. Detta gör att man har en kort tid på sig att återupprätta elkraftförsörjningen utan att telekommunikationerna störs. Om elavbrotten blir långvariga kan man få avbrott på grund av att batterierna laddar ur eller bränslet eller oljan i reservkraftsaggregaten tar slut. En utförligare diskussion rörande detta beroende finns i avsnitt 3.6.

[9] Skanova ingår numera i TeliaSonera.

Strävan idag är att centralisera och automatisera drift och underhåll för att på så vis spara på personalkostnader. För att hantera störningar hyr teleoperatörerna in entreprenörer. Vid stora störningar är det inte omöjligt att det uppstår brist på personal som har kompetens att utföra nödvändiga reparationer. Detta kan leda till att det tar lång tid att återupprätta telekommunikationerna efter avbrott.

I samband med krissituationer är det troligt att många abonnenter samtidigt vill utnyttja telefoner. Vid överbelastning kommer vissa samtal inte att kunna kopplas fram. Detta kan försvåra exempelvis för en krisledning som försöker koordinera insatser för att avhjälpa krisen. I dagens telenät finns ingen möjlighet att prioritera vissa abonnenters samtal utan alla behandlas med samma prioritet. Försök med prioritering av samtal har genomförts i PTS regi.

Utgående från dagens situation kan man konstatera att det fasta telenätet är robust vad det gäller slumpvisa störningar. En mycket väl underrättad angripare med tillräckliga resurser kan dock i princip på kort tid slå ut stora delar av det fasta telenätet. Det är då viktigt med god tillgång på kompetent personal och förberedda krisåtgärder. Det kan idag finnas brister i operatörernas beredskap att snabbt vid behov kunna samutnyttja resurserna i varandras nät.

## *3.3 Mobila telenät*

De mobila telenäten finns i olika varianter. Första generationens mobiltelefoni, till vilket man bland annat räknar NMT (Nordic Mobile Telephone ), är analogt. I Sverige dominerar idag andra generationens mobiltelefoni (2G), det digitala GSM (Global System for Mobile Communication). UMTS (Universal Mobile Telecommunications System) som utgör tredje generationen (3G) är under utbyggnad. Dessutom finns andra mobila telekommunikationssystem med mer specifika användningsområden.

Skillnaden mellan det mobila och det fasta nätet är huvudsakligen att mobilnätets accessnät är trådlöst och att det mobila nätet behöver funktionalitet för att lokalisera och identifiera abonnenterna.

Abonnenterna i ett telenät är registrerade i en databas. I det fasta näten görs detta i lokalstationerna. I de mobila näten kompliceras situationen av att man inte känner till var abonnenten kommer att ansluta sig till nätet.

Den trådlösa accessen sker med radiovågor vilket möjliggör rörlighet men sätter begränsningar på överföringskapacitet. Mobilnäten är cellulära. En cell är täckningsytan för radiovågor från en basstation. En basstation kan täcka flera celler genom att ha riktade antenner, till exempel i tre stycken 120°-sektorer. De frekvenser som används i en viss cell återanvänds i en annan cell längre bort. För att öka kapaciteten kan cellerna minskas så att frekvenserna kan återanvändas oftare. Mikroceller finns vanligen i stadskärnor och kan ha en radie på 100-300 m. I glesbygd finns stora celler med en radie på 30-40 km.

Gemensamt för alla mobila nät är att antalet samtidiga samtal inom ett visst område är begränsat. Det innebär att det ibland kan vara svårt att komma fram. Speciellt viktigt ur ett sårbarhetsperspektiv är att det vid större olyckor alltid genereras en stor mängd samtal inte bara från drabbade och krisledning utan även från oroliga och nyfikna.

### 3.3.1 Första generationen – NMT

I NMT (Nordic Mobile Telephony), som var det första kommersiellt gångbara mobiltelefonisystemet, ansluter sig de mobila terminalerna via basstationer och mobiltelefonväxlar till andra nät.

I Sverige är det endast Telia Mobile som tillhandahåller denna typ av mobiltelefoni och då i form av NMT 450. NMT450 hade 2001 endast 144 000 abonnenter. Dessa befinner sig till stor del i glesbygd där GSM-nätet i vissa fall kan ha begränsad täckning. Telias tillstånd att driva NMT 450 är nyligen förlängt och går ut den 31 december 2007. NMT baseras på samverkan med det fasta nätet och är anslutet med kopplingar mellan mobiltelefonväxlarna och förmedlingsnivån i Telias fasta nät.

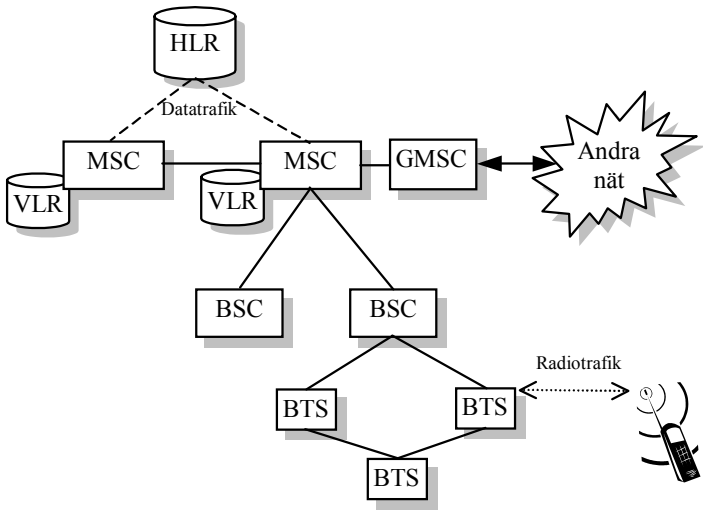
NMT är analogt och därför enkelt att avlyssna. NMT 450 använder sig av radiofrekvenser i 450 MHz bandet. Låga frekvenser har längre räckvidd och man kan alltså med färre basstationer täcka ett större område vilket är en fördel i glest befolkade områden.

Registrering av abonnenter är löst genom att olika nummerserier avsätts för olika växlar. Det medför att dessa växlar kan fungera autonomt vid avbrott i förbindelserna med andra växlar och inom sitt område hantera de abonnenter som finns registrerade där.

### 3.3.2 Andra generationen – GSM

Av de mobila kommunikationsnäten är idag GSM det dominerande. I Sverige finns för närvarande tre landstäckande GSM-nät vilka är i princip oberoende av varandra. Dessa drivs av Telia, Tele2 och Vodafone. Den 29 maj 2002 tilldelades dessutom SweFour ett fjärde nationellt GSM-tillstånd, med villkor att man senast i slutet av 2003 skall täcka minst 178 000 personer med egen infrastruktur.

GSM är tydligt uppdelat i olika hierarkiska nivåer med tillhörande noder. I den högsta nivån finns förmedlingsväxlar (MSC – Mobile Switching Centre) och transportnät till kontrollenheter för basstationer (BSC – Base Station Controllers). BSC styr basstationerna (BTS – Base Transceiver Station) som kommunicerar via radiovågor med mobilstationerna (mobiltelefonerna). GSM är anpassat för tre olika frekvensområden 900 MHz, 1800 MHz och 1900MHz. I Sverige används 900 MHz och 1800 MHz. De högre frekvenserna har kortare räckvidd men med bättre täckning inomhus varför de lämpar sig väl i städer.




Varje förmedlingsväxel kan ha ett eller flera trafikområden, och ett område kan hantera flera basstationsystem. Basstationssystemet kontrolleras av BSC:erna som avlastar MSC. Basstationer kan även ha egna förbindelser till MSC. Kopplingen mellan basstation och kontrollenhet kan utgöras av kabel eller radiolänk. Den kan också vara ringformad som i principskissen ovan.

I GSM-standarden har man valt att registrera abonnenterna i centrala databaser (HLR – Home Location Register). Detta ger stora fördelar ur effektivitets- och

rationalitetssynpunkt, men innebär att nätets funktion är beroende av att mobiltelefonerna kan nå de centrala databaserna.

HLR är vanligtvis samlokaliserad med en förmedlingsväxel men kan också vara fristående. Vid förmedlingsväxlarna finns också ett register över vilka abonnenter som för tillfället befinner sig i det område som kontrolleras av förmedlingsväxeln. Dessa register kallas Visiting Location Register (VLR). Kontakt med såväl HLR som VLR är nödvändiga för att samtal ska kunna kopplas upp. Det finns även andra centrala funktioner exempelvis servrar för behörighetskontroll eller tillhandahållande av exempelvis SMS-tjänster.

Förmedlingsväxlarna är anslutna till andra nät via så kallade gateways (GMSC – Gateway Mobile Switching Centre).

GSM är ett helt digitalt system med automatisk kryptering. Detta innebär bland annat avlyssningsskydd på radiokanalen mellan mobilstation och basstation och skydd mot obehörig lokalisering av mobilstationer. Dessutom möjliggörs integration av olika tilläggstjänster och anslutning av terminaler för fax- och datatrafik mm.

Telefonerna i GSM är i sig inte knutna till en viss operatör. Identitet och operatörstillhörighet ges av SIM-kort i telefonen.

GSM-näten har under det senaste året utökats med teknik för paketförmedlad trafik. Denna teknik, GPRS (General Packet Radio Service) med vidareutvecklingen EDGE (Enhanced Data Rate for GSM Evolution), innebär att man kan erbjuda datatjänster med överföringshastigheter på upp till 384 kbit/s. Pakettransmission gör det möjligt för abonnenten att vara ständigt uppkopplad till telenätet, abonnenten betalar för den mängd data som förmedlas inte uppkopplingstiden. Dessa påbyggnader går ibland under benämningen 2,5G.

### 3.3.3 Tredje generationen – UMTS

Tredje generationens mobiltelefoni, eller som den kallas i Europa UMTS, är under utbyggnad. PTS har beslutat att tilldela Vodafone, HI3G, Orange och Tele2 varsitt tillstånd. De har utfäst sig att till slutet av 2003 täcka in större delen av Sveriges befolkning.

I princip byggs idag två nät. Vodafone, Orange och Hi3G bygger ett nät och Tele2/Telia bygger det andra. På landsbygden och i glesbefolkade områden tillåter PTS att operatörerna samarbetar, i tätort skall de dock ha separata nät.

Arkitekturen och hierarkin av noder är densamma i UMTS som i GSM. UMTS är en global standard och förhoppningen är att samma telefon skall kunna användas för samma tjänster världen över. De närmaste åren kommer UMTS viktigaste bidrag vara att erbjuda högre överföringskapacitet för datatjänster och GSM kommer att fortsätta dominera för mobil taltelefoni. Men på längre sikt är det inte omöjligt att UMTS helt ersätter GSM.

Målet är att uppnå dataöverföringshastigheter på 114 kbit/s för en bilburen terminal, 384 kbit/s för fotgängare och 2Mbit/s i kontorsmiljö. Detta innebär att GSM med GPRS och EDGE kommer att existera som ett alternativ till UMTS för de lägre datatakterna.

På samma sätt som för GSM kommer intelligensen i nätet att vara koncentrerad till ett fåtal platser och telefonerna måste nå de centrala databaserna för att kunna upprätta en förbindelse.

UMTS använder frekvenser runt 2 GHz, detta innebär att räckvidden förkortas jämfört med GSM och NMT. Basstationer måste därför placeras ut mycket tätare.

### 3.3.4 Satellitbaserade system

I satellitbaserade system ersätter man de markbaserade radiobasstationerna med radiobasstationer på satelliter i banor runt jorden. Varje satellit täcker av en viss yta på jorden (satellite footprint). Två terminaler (satellittelefoner) inom samma satellittäckningsområde kan kommunicera direkt med varande via satelliten.

För kommunikation utanför en satellits täckningsområde måste samtalet vidarebefordras. Detta finns olika lösningar för att hantera dett, benämnda ”bent pipe architecture” och ”cross-linking architecture”. I ”bent pipe architecture” används en markbaserad gateway för att vidarebefodra samtal till en gateway som har kontakt med den satellit inom vilkens täckningsområde mottagaren befinner sig eller till det publika telenätet. I ”cross-linking architecture” sker kommunikationen direkt med andra satelliter. Cross-linking kräver inte en gateway i varje satellits täckningsområde.

Tekniska begränsningar för satellitsystem gäller framförallt kapacitet och reparationsmöjligheter. Antalet samtidiga användare begränsas av att kraftförsörjningen kommer från solpaneler och att varje satellit täcker en relativt stor yta. En annan begränsning är att satellittelefoner har problem att etablera och upprätthålla radiokontakt med sina satelliter inomhus och i stadsmiljö.

Kostnaden för anskaffning och utnyttjande av mobiltelefonsystem har minskat. Idag finns ett flertal satellitbaserade system. Exempel på dessa är Globalstar, Tiscali, Iridium och Inmarsat. Iridium som använder sig av cross-linking har ett sjuttiotal satelliter i funktion och tillhandahåller via IDG Europe AB global täckning. Inmarsat som har fyra satelliter i geostationär bana, använder bent pipe och täcker hela jorden utom polerna. Tiscali erbjuder bredbandsaccess via satellit.

### 3.3.5 Kommunikationsradio

Det finns ett stort antal enskilda radionät. I många fall är det fråga om små system, kanske bara en basstation som täcker ett visst område. Denna typ av system används i dag i stor utsträckning av polis, räddningstjänst och ambulanssjukvården.

Fördelen med en stor mängd enskilda system har varit att man kunnat anpassa funktioner och täckning efter de egna behoven. Det finns även nackdelar. Systemen är ofta bundna till enskilda leverantörer och det är dyrt att upprätthålla driften. Det är dessutom ett frekvensmässigt slöseri då speciella kanaler avsatts för varje enskilt system. Flera olika system försvårar dessutom samverkan.

Ett flertal av systemen närmar sig slutet av sin livslängd och det pågår för närvarande en debatt om ett gemensamt system som skall ersätta de gamla. Utredningar har utförts på uppdrag av regeringen 1997[10] och nu senast på uppdrag av näringsdepartementet[11]. En stark kandidat har varit det så kallade TETRA (TErrestrial TRunked Radio), en europeisk standard för radiokommunikation.

### 3.3.6 Mobitex

Mobitex är ett publikt paketförmedlande mobildatanät som specificerades av dåvarande Televerket och togs i bruk 1987. Systemet är avsett för text och data men tillåter även talkommunikation i begränsad utsträckning. Den frekvens som används är 66-88 MHz och datahastigheten är endast 1,2 kbit/s.

[10] SOU 1998:143 Ett tryggare Sverige. Ett gemensamt system för mobil kommunikation.

[11] Ett nät för trygghet - Rapport från Uppdrag Tetra radiokommunikation, Näringsdepartementet 2002

Vid uppbyggnaden hade Televerket ansvar för beredskapsfrågor och byggde Mobitexnätet med avsikt att det skulle fungera väl i krig.

Det finns sju huvudväxlar, 23 områdesväxlar och 219 basstationer.

Mobitex täcker 90% av Sveriges yta och 99,5% av Sveriges befolkning[12].

Fasta terminaler kan anslutas till områdesväxlar via fasta förbindelser. Mobila terminaler kommunicerar med systemets basstationer. Kommunikation med andra nät sker via huvudväxlarna.

Huvudväxlar, områdesväxlar och basstationer kan fungera autonomt vid avbrott i förbindelserna. Växlarna finns i bergrum eller i byggnader med splitterskydd. Det finns reservkraft på varje anläggning (minimum 10 timmar). Förbindelserna går i Telia Mobiles vanliga nät R-line. R-line är det förbindelsenät som Telia Mobile använder för alla sina nät. R-line bygger på hyrda förbindelser från Telia.

Försvarsmakten har givit bidrag till reservvägar i nätet och PTS har givit bidrag till reservkraft och vissa basstationer. Mot bakgrund av det minskade krigshotet och att Mobitex ses som ett föråldrat system har PTS och Försvarsmakten upphört att ge bidrag. Idag drivs nätet på kommersiella grunder och Telia Mobile avgör själv skyddsnivåer.

### 3.3.7 Sårbarheter i mobila telenät

Man kan konstatera att det finns en mängd olika telekommunikationsnät som stödjer trådlös uppkoppling. Detta i sig gör att det finns alternativa system om ett av dessa av någon anledning inte skulle fungera vid den tidpunkt eller den plats där en abonnent befinner sig. Ett problem är dock att varje nät kräver en egen variant av mobilterminal. NMT, GSM, UMTS, satellittelefoner och kommunikationsradioapparater opererar alla på olika frekvenser och på olika sätt. Inte ens inom ett enhetligt system som GSM där det i Sverige finns flera olika nät kan man obehindrat utnyttja dessa då operatörerna endast tillåter trafik från abonnenter som finns registrerade i just deras nät. Undantaget här gäller samtal till 112 som förmedlas oberoende av abonnentens operatörstillhörighet. Det skulle vara tekniskt möjligt att öppna GSM-näten så att operatörstillhörighet inte spelar någon roll. Detta skulle leda till en del problem vid återgång till normal drift. Det skulle krävas samordning mellan operatörerna och det finns idag inga förberedelser för att göra något sådant.

De flesta mobilterminaler är idag batteridrivna. I nyladdat tillstånd har de vanligen passningstider på 100 timmar eller mer och samtalstider på flertalet timmar. Det finns även gott om produkter som tillåter uppladdning av mobilterminaler via 12-voltsuttag i exempelvis en bil.

För kommunikationen mellan mobilterminalerna och basstationerna krävs att radiosignalerna är av tillräcklig kvalité annars kan samtalet störas eller brytas. Det maximala avståndet mellan en basstation och en mobilterminal påverkas av sändarstyrka och frekvens men även av eventuella hinder i vägen. Exempelvis kan räddningsarbeten i kuperad terräng, tunnlar eller byggnader försvåras av att man inte lyckas upprätta fungerande radioförbindelser.

I GSM identifieras den uppringande telefonen av basstationen vilket ska förhindra att obehöriga skaffar sig tillgång till nätverket. Däremot verifierar telefonen inte att den nått rätt nätverk. Med falska basstationer som överröstar de riktiga basstationerna är det möjligt att avlyssna eller störa trafiken inom ett område. I tredje generationens mobil-

[12] 2002-05-22 på http://www.mobitex.telia.com/

telefonisystem fungerar inte denna typ av basstationsattack då man lagt till funktioner som gör att telefonen kan identifiera sitt eget nätverk.

I det fasta telefonnätet vet man alltid hur många abonnenter som är anslutna till en viss lokalstation. I mobila nät kan abonnenterna förflytta sig och man kan alltså få fler abonnenter inom ett område än basstationerna klarar av att hantera. Denna situation kan även inträffa om en delmängd basstationer inom ett område slås ut. De återstående omkringliggande basstationerna kan då möjligen upprätthålla täckningen med kapaciteten minskar. Detta innebär att många abonnenter som teoretiskt skulle kunna upprätta radioförbindelse med en basstation ändå inte kommer att kunna komma fram eftersom basstationen redan är överbelastad. Denna typ av situation uppstod exempelvis vid elavbrottet i Kista år 2001 då basstationerna slogs ut när batterierna efter några timmar tagit slut.

Basstationerna utgör en relativt oskyddad del i de mobila telenäten. Av naturliga skäl bör de vara utspridda på platser som ger god täckning och placerade där det finns abonnenter. De är då troligen exponerade för vädrets makter eller personer som av någon anledning vill förstöra dem. Om enstaka basstationer upphör att fungera påverkas, som tidigare nämnts, snarare kapaciteten än täckningen. Bortfall av flera stationer inom samma område är allvarligare. Detta kan inträffa som ett resultat av målinriktade angrepp eller vid större elavbrott. Basstationer i GSM-nätet har batterireserver för avbrottsfri drift i minst 4 timmar (vissa operatörer har upp till 12 timmar) med möjlighet att koppla in reservkraftsaggregat. Från BSC och uppåt har man fasta reservkraftsaggregat.

Satelliterna som ju är en form av basstationer för satellittelefonsystem är däremot okänsliga för naturkatastrofer och självförsörjande på el. En angripare måste dessutom vara mycket resursstark för att kunna skada eller förstöra en satellit. Nackdelen är att om de går sönder så är satelliter svåra att reparera eller ersätta.

En skillnad mellan de olika mobila systemen är det antal basstationer som behövs för att täcka olika områden. UMTS utgör den ena extremen som kräver många basstationer då man vill ha hög bandbredd och dessutom använder höga radiofrekvenser i accessnätet. GSM kräver färre basstationer. NMT450 har ännu längre räckvidd och har därför bäst täckningsförmåga av de tre landbaserade publika mobiltelefonisystemen. Satellitbaserade system kan med mycket få satelliter täcka stora områden. Om man med färre basstationer täcker ett område får varje basstation en större betydelse för systemet som helhet. Ett system med många basstationer kan bli känsligare för långa avbrott i elförsörjningen då det krävs större resurser i form av personal och reservkraftsaggregat för att hålla basstationerna igång.

De mobila telenäten är beroende av ett transportnät, en nätinfrastruktur med hög överföringskapacitet. I avsnitt 3.5.1 förs en diskussion om sårbarheten i IT-infrastruktur med hög överföringskapacitet. Denna diskussion är till stor del även applicerbar på transportnätet i de mobila telenäten.

Det förekommer att de IT-system som utnyttjas för övervakning, styrning och administration av telekommunikationerna utnyttjar samma kommunikationsprotokoll som Internet (Internet protocol, IP). Många produkter är standardprodukter som används även i andra sammanhang. Särskilda åtgärder är därför nödvändiga för att styr- och övervakningsfunktioner, som är mycket viktiga delar i den logiska teleinfrastrukturen inte skall kunna utsättas för störningar i form av intrång och manipulationer.

Många datanät hos mobiloperatörerna är anslutna till Internet, bland annat för att ge tillgång till e-post och andra Internettjänster. Det förekommer också att man utnyttjar Internet för enkel åtkomst för underhåll och service m.m. Internetanslutningarna ökar

risken för dataintrång och virus vilket ökar möjligheterna att störa telekommunikationerna genom dataintrång eller riktade informationsoperationer.

I framför allt de digitala mobilnäten GSM och UMTS är beroendet av centrala databaser mycket stort. Om kontakten med dessa bryts eller om dessa slås ut upphör näten helt att fungera. Dessa databaser är därför normalt väl skyddade, speglade och har redundanta förbindelser. Den snabba utbyggnadstakten av GSM-näten under 90-talet innebar att det i vissa fall inte fanns tillräckligt med utrymme i bergrum för bland annat förmedlingsstationer (MSC) som därför fått placeras på andra platser. Att i efterhand flytta dessa till säkrare utrymmen är svårt och skulle kosta mycket pengar. En utslagen MSC skulle ge svåra problem. Det tar uppskattningsvis två dagar att koppla om trafiken och detta skulle ge kapacitetsproblem i nätet som drabbas. Att ersätta en MSC tar flera veckor.

## *3.4 Datakommunikation och IP-telefoni*

För datakommunikation är kretskoppling[13] ineffektivt eftersom data normalt kommer mycket ojämnt och kapacitet då reserveras i onödan. Istället använder man paketförmedlande teknik. Paketförmedling innebär att data styckas upp och sänds i paket. Flera samtal kan då använda samma förbindelse. Det finns olika protokoll som beskriver hur detta skall genomföras vilka har olika fördelar.

Det mest kända protokollet är idag IP (Internet Protocol) som är ett förbindelselöst protokoll. Det innebär att data som skall förmedlas delas upp i datapaket och att varje paket förses med en adress och skickas iväg. Det finns sedan inget som garanterar att paketen tar samma väg eller kommer fram i samma ordning som de skickades iväg. Detta skiljer sig från förbidelseorienterade protokoll vilka öppnar en förbindelse med ett uppkopplingspaket som innehåller adressen. De efterföljande paketen tar sedan samma väg som det första paketet och förbindelsen avslutas sedan med ett nedkopplingspaket. Även om IP är ett förbindelselöst protokoll använder det sig i sin tur vanligen av förbindelseorienterade protokoll för förmedlingen av sina paket.

Nät för datakommunikation har till stor del byggts nerifrån och upp, många gånger i avsaknad av starkare central styrning. Några datorer har kopplats ihop i ett lokalt nätverk. Detta nät har sedan kopplats ihop med en knutpunkt eller nät som tillhandahålls av en operatör. Utseende på och utrustning i de lokala näten kan därför variera stort, allt ifrån en enda dator med ett kabelmodem, till ett företagsnät med tusentals datorer, egna nationella förbindelser och en egen intern näthierarki.

Många enskilda användare hanterar idag sin interna datakommunikation via privata nät på separata förbindelser. Dessa är ofta hyrda från nätägare inom den svenska IT-infrastrukturen. I det följande redovisas de publikt tillgängliga kommunikationsformerna via Internet samt IP-telefoni.

### 3.4.1 Internet

Internet är ett världsomspännande virtuellt nät och består egentligen av tusentals fysiska nätverk baserade på IP som kopplats samman med hjälp av vägvalsdatorer (routrar). Denna sammankoppling görs på olika nivåer. När man talar om Internet menar man vanligen den publika delen av Internet som i princip är tillgänglig för alla. Privata nätverk baserade på IP är mycket vanliga. Från ett privat nät kan man vanligen komma åt Internet, medan man från Internet endast kommer åt de delar av det privata nätet som nätägaren valt att exponera.

[13] Kretskoppling se 3.1

Internet medger ett stort utbud av olika tillämpningar. De vanligaste och mest utnyttjade är e-post och WWW (World Wide Web).

Andra viktiga system och protokoll är DNS (Domain Name System) och NTP (Network Time Protocol). DNS konverterar logiska nummeradresser (IP-adresser) till mer lätthanterliga alfabetiska domännamn och e-postadresser. NTP medger att tidsinformation förmedlas i nätet och ger tillgång till en mycket exakt tid i varje ansluten dator. För DNS-systemets funktion finns speciella rotnamnservrar och namnservrar, liksom det finns tidservrar för NTP.

En internetoperatör bygger sitt nät runt ett stamnät. Detta baseras på komponenter (servrar, fiber, radiolänkar) och protokoll (exempelvis ATM, ISDN, X.25) som ger den kapacitet och geografiska utbredning som operatören önskar.

Genom att ansluta sig till olika knutpunkter får operatören kontakt med andra operatörers nät.

Internetoperatörens kunder kan ansluta sig direkt till routrar i stamnätet via fasta accesslinjer. Detta görs vanligen av myndigheter, större företag och lokala bredbandsoperatörer, men även av mindre företag och privatpersoner. Operatören kan också tillhandahålla någon form av accessnät (exempelvis kabel-TV-nät) som kunderna ansluter sig till. Med ADSL, modem och ISDN kan man använda det publika telefon-systemets accessnät för uppkoppling.

Trådlösa accessformer börjar bli vanligare. NMT, GSM och WLAN (trådlösa lokala nät) har funnits ett tag. Under utbyggnad är som tidigare nämnts GPRS och UMTS.

Det är vanligt att företag och myndigheter hyr fiberkapacitet, så kallad dedikerad linje, av nätoperatörer för att koppla ihop de företagsinterna datanäten i olika landsdelar.

### 3.4.2 IP-telefoni

IP-telefoni är en tillämpning som bygger på att man använder IT-infrastrukturen och IP-protokollet, för att förmedla tal. Det innebär att abonnenten har en egen dator eller terminal som digitaliserar talet och omvandlar det till IP-paket som sedan skickas iväg över datanätet. Fördelarna med detta är bland annat att man kan använda samma nätinfrastruktur för såväl tal som data.

IP-telefoni för publikt bruk över Internet förekommer än så länge endast i liten utsträckning. Det finns tekniska problem då taltrafik är mycket känsligt för fördröjningar och möjligheterna att prioritera tal på Internet är begränsade. I takt med att bandbredden i näten ökar kommer kvalitén att förbättras och fler att använda IP-telefoni. I dagsläget används IP-telefoni huvudsakligen för kommunikation inom större företag och myndigheter som förfogar över ett eget datanät. Trafiken behöver då inte passera över den publika delen av Internet och det blir lättare att garantera kvalitén.

### 3.4.3 Sårbarheter hos Internet och IP-telefoni

Varje terminal eller apparat som ansluts till Internet och tilldelas en IP-adress kan interagera med andra anslutna enheter. Detta är själva poängen, men innebär även att man exponerar enheten för aktörer med illasinnade avsikter. Det finns idag många system för att skydda sig mot detta, exempelvis behörighetssystem, brandväggar, anti-virusprogram och IDS (Intrusion Detection System). Denna typ av system ger normalt ett relativt gott skydd. Den vanligaste orsaken till att man misslyckas med att hålla illasinnade aktörer borta är att dessa system inte är rätt konfigurerade och uppdaterade. Större företag och myndigheter

kan ofta ha personal som på heltid ägnar sig åt detta. Mindre företag och privatpersoner är däremot vanligen mer oskyddade.

När det finns många system med låga säkerhetsnivåer får den som vill störa de elektroniska kommunikationerna goda möjligheter att verka anonymt med stor genomslagskraft. Att använda oskyldiga användares datorer som plattformar för angrepp gör att angriparen blir svårare att spåra. Genom att ta över ett stort antal datorer går det att initiera överbelastningsattacker mot system som är av större vikt för samhället.

Stora företag som anser sig ha god säkerhet kan också exponera sig när man i affärssyfte kopplar ihop sina system med små företag som har sämre säkerhet i sitt lokala nät.

System som är extremt kritiska för en verksamhet bör man överväga att helt frikoppla från Internet för att undvika IT-attacker och intrång. Inte ens detta hjälper alltid. Okunnighet, slarv och misstag kan göra att någon av misstag kopplar systemet till Internet eller för över illasinnad kod via en smittad diskett eller CD-skiva.

IP-telefoni är till skillnad från fast telefoni känslig för störningar i abonnentens elförsörjning. Om strömmen försvinner hemma hos en abonnent kommer strömförsörjningen till abonnentens terminal att försvinna och således även möjligheten att använda terminalen för telefoni.

De lokala nätverken börjar i allt större utsträckning även använda radioförbindelser. Detta medför säkerhetsproblem då det underlättar för utomstående att obemärkta koppla upp sig mot eller avlyssna trafiken i nätet.

Internet och IP-telefoni är beroende av den svenska IT-infrastrukturen med hög överföringskapacitet. Sårbarheten i denna diskuteras närmare i avsnitt 3.5.1.

Det bör även nämnas att IP är konstruerat för att smidigt kunna utnyttja redundanta förbindelser och således är mindre sårbart för avbrott. Det är ibland svårt att avgöra om alternativa vägar i trafiken verkligen innebär alternativa fysiska vägar då många operatörer kan ha fiber i samma kanalisering. Varje kabel innehåller flera fibrer och skada på en kabel kan medföra störningar i flera operatörers nät. Det är alltså inte säkert att man får en minskad sårbarhet för avbrott i förbindelser även om man skulle anlita flera operatörer.

Det dynamiska sätt på vilket datapaketen färdas över Internet medför att varken mottagare eller avsändare har någon större kontroll över vilka mellanhänder som passerats på vägen. Det finns metoder för att relativt säkert kunna garantera att avsändare och mottagare är de som de utger sig för att vara och att innehållet i paketen stämmer med det som skickades iväg.[14] Användandet av denna typ av metoder är ännu så länge relativt omständligt vilket gör att det kanske inte används i tillräcklig omfattning. Det krävs dessutom en infrastruktur i form av pålitliga organisationer som tillhandahåller de certifikat som behövs och kan tillhandahålla servrar som verifierar giltigheten i certifikaten. Denna typ av servrar utgör en sårbarhet i sig då bortfallet av en server skulle kunna medföra att säker kommunikation omöjliggörs.

För Internet finns i Sverige fyra stycken nationella knutpunkter för trafikutbyte. Dessa är lokaliserade till Stockholm, Malmö, Göteborg och Sundsvall. Samplacerat med dessa är tidservrar och namnservrar liksom en av världens tretton rotnamnservrar. De nationella knutpunkterna finns placerade i bergrum, med dubblerad utrustning och redundanta förbindelser och drivs av Netnod i samarbete med Sveriges Internetoperatörers Forum (SOF). Operatörer kan även ha egna knutpunkter där de utbyter trafik med varandra. I

[14] Exempel på detta är PKI (Public Key Infrastructure)

vilken utsträckning det finns sådana är i dagsläget oklart, dock skulle det ha en positiv påverkan på nätets förmåga att klara störningar.

En Internetoperatör behöver inte utnyttja knutpunkter i Sverige utan kan leda sin trafik till knutpunkter i utlandet. Detta kan naturligtvis vara en fördel då kunderna kan ha en bibehållen förbindelse även om de svenska knutpunkterna skulle fallera. Men omvänt kan kunden drabbas av störningar relaterade till hot som svenska knutpunkter är skyddade mot.

Utslagning av en eller flera knutpunkter medför att trafiken mellan operatörer störs. Enskilda operatörer kan då förlora kontakten med Internet. Att slå ut knutpunkter, tidservrar, rotnamnservrar och namnservrar fysiskt får anses som svårt. Troligare är angrepp i form av överbelastningsattacker som resulterar i att servrarna görs otillgängliga. Man kan även tänka sig intrång i syfte att förstöra eller manipulera den information som servrarna tillhandahåller.

Om man lyckas slå ut ett flertal rotnamn- eller namnservrar under en längre tid kan detta leda till att hela eller delar av Internet i princip stängs ned för normal användning då uppslagningen av adresser slutar att fungera. Kortare avbrott får inte samma effekt då datorer oftast lagrar tidigare uppslagningar en viss tid.

Tillgång till korrekt tid är av stor vikt för många säkerhetsfunktioner för att exempelvis kunna garantera att ett certifikat är aktuellt eller för att spåra intrång genom att titta på tidstämplar i olika loggar. Det är även viktigt vid synkronisering av data då man vill veta vilken information som ändrades senast. Tidservrarna synkroniserar sina klockor mot det amerikanska satellitnavigeringssystemet GPS (Global Positioning System) och är därför i viss grad beroende av detta system.

## 3.5 IT-infrastruktur med hög överföringskapacitet

Någon officiellt fastställd definition av IT-infrastruktur med hög överföringskapacitet finns inte. Vanligen menas dock en förbindelse för elektronisk kommunikation som medger förmedling av stora informationsmängder på kort tid och med förutsättning att överföra rörliga bilder och ljud med god kvalitet. I denna infrastruktur ingår nät baserade på optiska fibrer, kopparkabel och radiolänk. Dessutom ingår vägvalsutrustning (routrar) och signalförstärkningsutrustning. Att kunna överföra rörliga bilder och ljud kräver även åtgärder i nätinfrastrukturen för att garantera att gränsvärden för maximal fördröjning och paketförluster inte överskrids.

Bredbandsutredningens indelning i nationellt stamnät, ortssammanbindande nät, områdesnät och fastighetsnät utgör en hierarkisk indelning av IT-infrastrukturen.[15] Det nationella stamnätet utgörs av rikstäckande allmänt tillgängliga nät som förbinder nationella noder och huvudnoder i landet med varandra. Detta nät sammanfaller ofta med det ortssammanbindande nätet som förbinder orter med varandra. I orterna anses det sedan finnas ett områdesnät som sammanbinder fastighetsnäten med det ortssammanbindande nätet. Fastighetsnäten på lägsta nivån är det nät som förbinder lokalerna i samma fastighet. Denna indelning skall bland annat hjälpa kommunerna att få en enhetlig terminologi i sina IT-infrastrukturplaner. Det kan ibland vara svårt att dra gränsen mellan vad som exempelvis är ortssammanbindande och nationellt stamnät.

Näten på högre nivå (nationellt stamnät och ortsammanbindande nät) utgörs av fiberoptiska kablar och radiolänkar. De fungerar också som transportnät för fast och mobil telefoni. Telia, Banverket, Utfors och Svenska Kraftnät har idag nationella fibernät som, tillsammans med de kommunala näten, i princip täcker hela landet. Denna fiber är oftast

[15] SOU 2000:111, IT-infrastruktur för stad och land, s. 175 och framåt.

dragen längs vägar, banvallar och i kraftledningsstolpar. Teracom kompletterar med ett radiolänkbaserat nät med liknande utsträckning. Detta innebär att det i landet finns ett flertal fysiskt och operatörsmässigt skilda nät. Idag har alla av landets kommuner minst en och 75 % minst två nätoperatörer med anslutningspunkter till stamnätet.[16]

### 3.5.1 Sårbarheter i IT-infrastrukturen

Optiska fibrer är inte känsliga för elektromagnetiska vapen, däremot behövs separat elförsörjning för att driva den optiska förstärkarutrustning som krävs. Radiolänkar kan störas ut med störutrustning. Avbrottet pågår då så länge störsändning pågår. För mer permanent avbrott krävs att man förstör själva radiolänkstationen.

Operatörer köper kapacitet i andras nät för att komplettera sina egna. Man köper dock i regel inte extra förbindelser i akuta situationer. Istället försöker man koppla runt avbrottet i de redan tillgängliga förbindelserna. Detta klarar man normalt på mindre än 12 timmar. För Försvarsmaktens behov har PTS även upphandlat hopkopplingspunkter tänkta att kunna förbättra möjligheterna för operatörer att utnyttja varandras nät i händelse av avbrott. Hopkopplingspunkternas begränsade kapacitet och affärsmässiga hänsyn gör att det finns anledning att ifrågasätta om den samlade redundansen skulle utnyttjas effektivt vid svåra påfrestningar i fred. En kapacitetsförstärkning och ökad samverkan mellan operatörer för utnyttjande av tillgängliga förbindelser i flera nät skulle kunna förbättra flexibiliteten och redundansen i de nationella stamnäten.

Hantering av allvarliga fel och störningar i IT-infrastrukturen kräver personal med hög kompetens. Det finns få sådana specialister i Sverige idag vilket kan försvåra och försena en återuppbyggnad vid skador på IT-infrastrukturen.

Av kostnads- och effektiviseringsskäl strävar operatörerna efter att automatisera och centralisera drift och övervakning. Med allt öppnare gränser innebär detta att många internationella operatörer kan komma att förlägga sina driftcentraler utomlands, men även omvänt att vilja förlägga centrala noder, viktiga för andra länder, i Sverige.

Den snabba tekniska utvecklingen inom detta område gör att utrustningen snabbt blir omodern. Det blir allt för dyrt att hålla reservutrustning i lager. Detta kan göra att en återuppbyggnad efter fysiska skador tar längre tid.

## *3.6 De elektroniska kommunikationernas beroende av el*

Beroenden mellan el- och telesystem vid omfattande och långa elavbrott analyserades under 2001 av Svenska Kraftnät i samråd med PTS.[17] [18]

De elektroniska kommunikationsnäten är helt beroende av el för att fungera. Avbrott i elförsörjningen på upp till ett par timmar klarar man normalt då de flesta noder i telenäten är försedda med batteribackup. Centrala noder klarar sig normalt ännu längre då de dessutom ofta har reservkraft i form dieselgeneratorer. Ett av de vanligaste problemen anges av operatörerna dock vara elavbrott.

För det fasta telenätet är lokalstationer och förmedlingsstationer utrustade med egen reservkraft bestående av batteri och dieselgeneratorer. Mindre anläggningar som utbrutna

[16] IT-infrastrukturen i Sverige, 2002 – Tillgänglighet i olika delar av landet. PTS-ER-2002:20

[17] Beroenden mellan el- och telesystem vid omfattande och långa elavbrott, Svenska Kraftnät, 25 oktober 2001

[18] Säker elförsörjning för telefunktionen, PTS, 29 oktober 2001

abonnentsteg har endast batterireserv med 4 till 8 timmars uthållighet, den kortare tiden i tätort och den längre utanför.

För det mobila telenätet är gateways (GMSC), växlar (MSC) och kontrollenheter för basstationer (BSC) utrustade med reservkraft i form av batteri och dieselaggregat. Radiobasstationerna har dock vanligen endast 2-5 timmars batterireserv. Denna tid kan dock vara kortare eller längre beroende på batterikvalitet, batterikapacitet och trafikbelastning. Vid längre avbrott kan man vanligen behålla viss täckning utomhus men kapaciteten i de mobila näten reduceras. Detta beror på att en mindre andel basstationer även är anslutna till reservaggregat. Detta observerades till exempel vid elavbrottet i Kista/Akalla den 11 mars 2001.

Vid överföring längre sträckor via optisk kabel (mer än 5-10 mil) sker förstärkning av signalerna i förstärkarpunkter. Dessa är beroende av elkraft. Många av dessa punkter är försedda med batterireserver på 2 till 4 timmar. En del har även dieselreservkraft alternativt intag för mobil reservkraft. Utbyggnaden av optisk fiber har dock i vissa fall gått så fort att det ibland saknas reservkraft.

Den utrustning som ägs och hanteras av tele- och Internet-operatörerna är således utrustad med reservkraft att klara kortare och i viss utsträckning längre elavbrott. Däremot har deras kunder ofta brister i sin utrustning. Företagsväxlar, servrar och trådlösa så kallade DECT-telefoner är beroende av elförsörjning. Så även om operatörerna lyckas hålla sin utrustning igång så är risken stor att man inte kan utnyttja detta.

PTS har upphandlat 1600 reservkraftsaggregat som fördelats bland teleoperatörerna. Utnyttjandet av dessa aggregat regleras i avtal mellan operatörerna och PTS. Det anses allmänt att detta har reducerat störningar i samband med elavbrott i såväl fasta som mobila nät. Operatörerna anser sig inte kunna hantera fler aggregat på ett smidigt sätt varför tillförandet av ytterligare aggregat inte kan väntas ge ytterligare reducering. Eventuellt skulle mer samplanering mellan teleoperatörerna kunna leda till att de aggregat som finns idag kan utnyttjas effektivare vid en större störning.

Reservkraftsaggregaten kräver regelbunden tillsyn. Då de inte är i bruk måste man provköra och underhålla dem. När de används kräver de tillsyn flera gånger per dygn. De måste regelbundet tankas. Kontinuerlig drift sliter på reservkraftsaggregaten och det finns risk att de skär. Det är därför viktigt att man byter olja minst vart tredje dygn.

Utplacering, omgruppering, tillsyn och tankning av reservkraftsaggregat kan i krissituationer vara besvärligt. Då stora områden drabbats krävs mycket personal. Ett stort problem kan vara att skaffa fram fordon som kan ta sig fram i området. Framkomligheten kan vara begränsad till exempel på grund av stormfälld skog eller översvämningar. Nattetid kan det vara svårt att orientera sig då vanliga landmärken och riktmärken är nedsläckta. Mobiltelefonnätens basstationer kan stå otillgängligt på exempelvis tak vilket kan göra det svårt att koppla in reservkraftverk. Aggregaten liksom eventuella lager av bränsle nära dessa medför ökad brandfara.[19]

Erfarenhet visar också att reservkraftsaggregaten är mycket stöldbegärliga. Detta noterades i samband med kabelbranden i Kista men även isstormen i Kanada utgör ett exempel på detta.[20]

Vid elavbrott behövs alltså inte bara personal för underhåll utan även för bevakning av reservkraftsutrustning. Det är inte otroligt att det uppstår en brist på personal med el-

[19] Elavbrotten i Auckland, Totalförsvarets Forskningsinstitut, maj 2001, FOI-R--0102--SE

[20] Isstomen i Kanada, Totalförsvarets Forskningsinstitut, maj 2001, FOI-R--0103--SE

kompetens i en krissituation då stora områden och många operatörer drabbas. Man riskerar då att få utarbetad personal med extra risk för att misstag begås och olyckor inträffar.

En metod för att upprätthålla viss strömförsörjning även om tillgången måste ransoneras är att periodvis koppla bort elförsörjningen till vissa områden, ibland benämnt roterande bortkoppling (RoBo).[21] Detta innebär att man slår av elförsörjningen till ett visst område under en viss tid varje dygn. Erfarenheter från exempelvis kriget i Jugoslavien där Natos bombningar störde elförsörjningen visar att detta gav problem även för telefonnäten. För att upprätthålla viss elförsörjning införde man RoBo med 6 timmars elförsörjning och 18 timmars avbrott per dygn. Telefonnätens noder med batteribackup slogs ut ett fåtal timmar efter det att strömmen brutits. Under de timmar man hade el var denna dessutom av mycket varierande kvalitet, man hade bland annat svårt att hålla rätt spänning och frekvens på växelströmmen. Detta innebar att uppladdningen av batterierna försvårades. Ibland innebar den dåliga el-kvalitén till och med att utrustning skadades.[22]

En av de vanligaste orsakerna till avbrott i teletrafiken under fredstid är just avbrott i elförsörjningen. Teleoperatörerna är medvetna om detta. I den utsträckning en ökad tillförlitlighet i elförsörjningen alls är möjlig att köpa från elbolagen så anser man dock från teleoperatörernas sida att priset idag är för högt. Detta förhållande anses av de inblandade ha minst två orsaker. Dels att elbolagen inte på ett enkelt sätt idag tekniskt kan erbjuda el med högre tillförlitlighet för vissa abonnenter. Men även på att elbolagen inom sina koncessionsområden har en monopolsituation och att därför saknar intresse av att erbjuda denna typ av tjänst. I stor utsträckning har man också anpassat sig till detta och med PTS hjälp, utformat sina system för att klara avbrott i elförsörjningen. En tydligare samverkan mellan el- och teleoperatörer är nödvändig för att reducera risken för allvarliga konsekvenser i samband med elavbrott.

## 3.7 Framtida sårbarheter

Vi ser idag är en tillväxt av Internet och mobiltelefoni. Detta innebär att vi får fler personer som förlitar sig på denna infrastruktur och gör sig beroende av att den fungerar samtidigt som man överger gamla system och tekniker. Traditionellt har vi i Sverige haft en hög nivå av säkerhetstänkande. Tidigare hade vi en tydligare hotbild vilket gjorde att incitamenten att beakta säkerhet och sårbarhet var hög. Det fanns också mer tid och ekonomiskt utrymme att ta hänsyn till säkerhetsfrågor. Idag är lönsamhets- och effektiviseringskrav en större drivkraft och det finns mindre utrymme att göra sådant som inte direkt främjar affärerna. Det finns därför en risk att användare av dessa nya infrastrukturer förlitar sig på att de alltid skall fungera och inte reflekterar över alternativ.

Telefoni och datatrafik konvergerar allt mer i näten. De stamnät som finns förmedlar inte bara det ena eller det andra. Digitaliseringen gör också att det kan vara svårt att skilja det ena från det andra. Denna konvergens syns allt mer även i accessnäten. ISDN och ADSL gör det möjligt att effektivt utnyttja kopparnäten för överföring av data. Detsamma sker i mobilnäten med ankomsten av GPRS och UMTS. Likaså tränger taltelefoni in i datatrafiken då IP-telefoni används i större utsträckning. Detta innebär att sårbarheter i IT och telefoni blir allt mer synonyma och svårare att skilja åt. Det innebär också att de olika systemen kan utnyttja varandras infrastrukturer och på så vis få en ökad tillgänglighet.

[21] Svenska kraftnät använder inte begreppet RoBo utan pratar istället om manuell frånkoppling (MFK). Ofta förutsätter man att MFK genomförs som en roterande bortkoppling, RoBo. Därför används begreppen MFK och RoBo ibland synonymt.

[22] Jugoslavienkriget 1999. Infrastrukturen i skottlinjen, Totalförsvarets Forskningsinstitut, augusti 2001, FOI-R--0544--SE

Även terminalerna integreras med varandra i större utsträckning. I framtiden är det möjligt att varje person har sin personliga terminal (kombinerad telefon och handdator) och att denna kopplar upp sig på det för tillfället mest ekonomiska och effektiva sättet. En effekt blir troligtvis ett ökat beroende av fungerande elektronisk kommunikation. En annan att man får ett effektivare utnyttjande av den samlade redundansen i systemen. Om exempelvis den snabba kopplingen via UMTS inte fungerar av någon orsak kopplar terminalen automatiskt över till att försöka via GPRS/GSM.

De senaste åren har det skett en kraftig utbyggnad av näten med optisk fiber. Detta beror på en medveten satsning från statsmakternas sida, men även på ett krav på ökad bandbredd. Detta krav har bland annat drivits på av utbyggnaden av tredje generationens mobiltelefoni som förväntas generera mer trafik och således kommer att kräva mer kapacitet i stamnäten. Med rätt planering kan denna utbyggnad ge en ökad redundans i näten. Den senaste tidens minskade utvecklingstakt inom telekomsektorn har dock medfört att det idag på många områden finns ett överutbud av fiberkapacitet.

Driften av de elektroniska kommunikationsnäten är redan idag i stor utsträckning centraliserad och automatiserad. Detta ger god ekonomi och effektivitet för operatörerna och man kommer troligen att försöka centralisera och automatisera ännu mer. Detta har både positiva och negativa effekter på sårbarheten. Det är positivt då operatörerna snabbt kan agera på störningar och har en god överblick över nätens aktuella status. En negativ effekt kan vara att färre personer finns till hands då någonting händer. Det är dessutom troligt att färre personer har kännedom om systemen.

Något man måste beakta är att många operatörer idag inte bara har sin verksamhet förlagd i Sverige. Redan idag finns driftcentraler i Sverige som styr och övervakar nät i andra länder. Det är troligt att man kommer att få fler internationella driftcentraler som styr över näten i flera länder. I svenska driftcentraler kan man behöva ha beredskap för hantering av kriser utomlands och omvänt kan det finnas behov av en beredskap att från svenskt håll samverka med driftcentraler utanför landets gränser.

Den tekniska utvecklingen går mycket snabbt och tekniker och standarder avlöser varandra. De senaste åren har telekommunikationsbranschen dessutom skakats av en strukturell, ekonomisk och finansiell oro såväl utomlands som i Sverige. I denna situation är det inte troligt att sårbarheten vid svåra påfrestningar är det område som branschens aktörer ger högst prioritet.

# 4 Risker för samhället

De elektroniska kommunikationerna spelar idag en omfattande roll för i stort sett alla samhällsfunktioner. En fullständig eller samlad bild är svår för att inte säga omöjlig att sammanställa. Man kan dock konstatera att beroendet är stort och att det hela tiden ökar.

I det följande kommer vi att redogöra för några uppenbart viktiga samhällsfunktioner och deras systemberoende idag. Exempel på sådana funktioner kan vara: polis, sjukvård, betalningsväsende, varudistribution och transporter, myndighetsutövning, näringsliv (handel, produktion, processtyrning).

Avbrott i de elektroniska kommunikationerna kan ge mer eller mindre allvarliga konsekvenser och vi kommer att ge några exempel.

Återkommande störningar kan skada människors förtroende för system och samhälle.

## *4.1 Risker i vardagen*

Vi använder oss idag i allt större utsträckning av elektronisk kommunikation i vårt dagliga liv. I princip alla svenska hushåll har idag fast telefon och en allt större andel är anslutna till Internet. En stor del av befolkningen är ständigt nåbar på mobiltelefon.

I och med att dessa system har visat sig lätta att använda och mycket pålitliga så förlitar sig människor i allt större utsträckning på dessa system. Det kan exempelvis yttra sig så att man inte bestämmer exakt tid och plats för möten utan räknar med att kunna ringa och bestämma mer exakt lite senare.

För den enskilde personen innebär avbrott i telekommunikationerna kanske vanligen inte mer än att man får ringa senare eller att man tvingas gå eller åka och besöka den person man ville tala med. Vissa saker blir mer omständliga och tar mera tid att utföra.

### 4.1.1 Näringsliv och myndigheter

Näringsliv och myndigheter använder sig i stor utsträckning av telefon, fax, Internet och e-post för att kommunicera internt och externt. Man använder sig av mobiltelefon för att kommunicera med personal som jobbar ”ute på fältet”. Fax och e-post används för att diskutera, informera och kommunicera. Internet används för att nå en bredare publik med information. Man har så kallade intranät för att informera den egna personalen och extranät för att informera sina kunder/medborgare.

Detta är en utveckling som uppmuntras och eftersträvas. Exempelvis så jobbar man idag för den så kallade 24-timmarsmyndigheten, det vill säga att svenska myndigheter med hjälp av elektronisk kommunikation skall vara tillgängliga 24 timmar om dygnet 7 dagar i veckan.

Många företag har idag datoriserade order, lager, faktureringssystem som är direkt beroende av fungerande system för elektronisk kommunikation. Genom datakopplingar till sina underleverantörer kan ett företag automatiskt lägga order på komponenter i samma ögonblick som de själva får en order från sina kunder. Detta gör att man kan minska lagerhållning och öka effektiviteten.

Elektronisk kommunikation är även viktig inom industrin för processtyrning, larm- och övervakning och inom vattenförsörjningen där man styr och övervakar dammar, luckor och pumpar.

För varudistribution och transporter är speciellt de mobila telenäten av stor vikt. Man vill utnyttja sin flotta av transportfordon så effektivt som möjligt. Mobila telekommunikationer

öppnar för större möjlighet och flexibilitet att dirigera fordonen som man vill. Inom exempelvis drivmedelsförsörjningen används det publika telenätet för att kommunicera från åkare till drivmedelsbolag till drivmedelsdepåer.

Trots att man idag är mycket beroende av elektronisk kommunikation inom näringsliv och myndigheter så klarar man ofta av att hantera kortare avbrott, även om detta kan leda till frustration och förseningar.

Vid längre avbrott kan man tvingas att övergå till manuella rutiner. Till exempel skicka magnetband per post istället för att skicka data över elektroniska kommunikationskanaler. Denna typ av omställning tar ofta tid och är mindre effektiv vilket innebär ökad arbetsbelastning och stress för personal.

Givetvis kan det även leda till ekonomiska förluster. På grund av ökade personalkostnader men även då exempelvis produktionskritiska komponenter tar slut och man inte lyckas beställa nya i tid med produktionsstopp som följd.

Stora störningar i näringslivets system för elektroniska kommunikationer kan efter hand leda till svåra påfrestningar på samhället i fred.

### 4.1.2 Betalningar

Sveriges betalningssystem är mycket beroende av fungerande elektroniska kommunikationer. De olika aktörerna i betalningssystemet, Riksbanken, affärsbankerna, VPC AB, Stockholmsbörsen och BGC, överför varje dag mycket stora belopp mellan varandra. Detta datautbyte sker till största delen via fiber som man hyr av teleoperatörerna. Likaså sker en stor del av betalningarna i handeln numera via betalkortsterminaler som är beroende av de publika telenäten.

Avbrott i de elektroniska kommunikationerna leder till stora problem då antalet transaktioner som hanteras är mycket stort och det i många fall skulle vara omöjligt att behandla dessa med manuella rutiner.

Fallet betalningar demonstrerar dessutom med tydlighet att tillförlitligheten är minst lika viktig. Det är stora värden som transporteras. Brottslingar kan avsiktligt vilja förvanska information, avsändare eller mottagare för att på så sätt lura till sig pengar vilket kan leda till stora direkta förluster. I förlängningen kan en osäkerhet i huruvida innehåll, avsändare eller mottagare är riktig minska förtroendet till de elektroniska betalningssystemen.

Osäkerhet och störningar i handelns elektroniska betalningssystem kan leda till att större mängder kontanter används, med manuella rutiner och ökade kostnader som följd, men även med ökad risk för brottslighet.

Om större störningar skulle uppstå kan förtroendet för betalningssystemet minska. Detta är mycket allvarligt då stabiliteten i ekonomin till stor del beror på de olika aktörernas förtroende för varandra. Stora störningar i betalningssystemet skulle kunna leda till att vi får en situation som innebär en svår påfrestning på samhället.

## *4.2 Risker vid svåra påfrestningar*

Ett enstaka avbrott i elektroniska kommunikationer under begränsad tid leder normalt inte till en svår påfrestning på samhället. Det kan dock få svåra följder om en viktig samhällsfunktion drabbas eller om avbrottet inträffar i och förvärrar en redan pågående kris. Som påpekats tidigare skulle bristande elektronisk kommunikation få svåra konsekvenser för exempelvis industriell verksamhet, handel och betalningsväsende. I det följande ger vi exempel på vikten av fungerande kommunikationer och redovisar sedan några samhällsviktiga funktioner och deras beroende av elektronisk kommunikation.

Krishantering kan ske på olika sätt och med olika metoder. Det bästa är om man kan förhindra att en kris uppstår eller åtminstone upptäcka den så tidigt att man kan lindra dess effekter. Detta är dock inte alltid möjligt och när en kris väl har uppstått måste den hanteras på något sätt. Det är då viktigt att man har i förväg uppgjorda planer, rutiner och tillgängliga reservsystem. I efterhand vill man troligen i görligaste mån återställa förhållandena till någon form av normalläge.

I de förebyggande och förberedande faserna är det viktigt att man tar hänsyn till telekommunikationerna. I det akuta skeendet och i samband med återuppbyggnaden är det till mycket stor hjälp om man har fungerande telekommunikationer.

Akuta situationer kommer att uppstå då man snabbt behöver få fram rätt information till rätt personer. Då stora geografiska områden och många människor drabbas samtidigt i kombination med omfattande materiella skador är det dessutom troligt att det uppstår brist på insatsresurser för att hantera problemen. Detta ställer ytterligare krav på goda telekommunikationer för att på effektivaste sätt kunna prioritera och koordinera insatser.

Vid höjd beredskap och krig är totalförsvarets elektroniska kommunikationer av avgörande betydelse. Försvarsmaktens utveckling mot ett nätverksbaserat försvar understryker detta än mer.

### 4.2.1 Erfarenheter från Kanada och Nya Zeeland

Den isstorm som drabbade östra Kanada i början januari 1998 ger många exempel på hur betydelsefulla telekommunikationer är i en akut krissituation och hur pass sårbara dessa är för extremt väder och störningar i elförsörjningen.

Mellan den 4 och 10 januari 1998 drabbades östra Kanada av en isstorm som så småningom skulle komma att kallas den värsta i modern kanadensisk historia. På grund av en extrem isbildning på elledningar m.m. uppstod mycket omfattande skador på elnätet i provinserna Québec och Ontario, där som mest över 1,6 miljoner abonnenter var utan elförsörjning. Elavbrottet drabbade en stor del av de 5,5 miljoner människor som bodde i området. I vissa områden varade elavbrotten i nästan fyra veckor, huvuddelen av de drabbade, ca 90 procent, fick dock tillbaka elströmmen efter två veckor. Det krävdes mycket omfattande insatser från hela samhället för att hantera situationen, bland annat fick man organisera tillfälliga nödförläggningar för närmare 100 000 personer. Under isstormens kulmen hade t.ex. den kanadensiska försvarsmakten satt in mer än 16 000 man i olika hjälpinsatser, vilket är den mest omfattande humanitära fredstida insatsen av militär personal i Kanada.

Även telekommunikationerna utsattes stora påfrestningar. Isstormen i sig innebar att telekommunikationernas fysiska strukturer, så som master och stolpar, skadades eller kollapsade. Dessutom bildades tjocka lager is på mikrovågsantenner och mobiltelenätens antenner. Detta följdes av att elförsörjningen slogs ut, vilket i sin tur påverkade telekommunikationerna. Televäxlar och liknande komponenter kunde visserligen drivas med elkraft från batterier, men dessa behövde återuppladdas vilket krävde reservkraftsgeneratorer. Generatorerna var man tvungna att skaffa i konkurrens med ett stort antal företag och andra organisationer som också hade behov av reservkraft.

För den största teleoperatören i det drabbade området, Bell Canada, innebar isstormen utslagning av uppskattningsvis 400 televäxlar, en trefaldig ökning av samtal till reparations- och operatörstjänster, reparation och/eller byte av ca 230 000 nedfallna telefonledningar, byte av 8 000 telefonstolpar, byte av 700 km kopparkabel och 50 km optisk fiber samt insats av 2 100 tekniker för reparation av telesystemen. Dessutom behövde man etablera två krisledningscentra för att övervaka olika aktiviteter som var

relaterade till isstormen. Den totala, oförutsedda och oförsäkrade ekonomiska kostnaden för Bell Canada översteg 110 miljoner kanadensiska dollar. Tack vare en god krishantering lyckades man trots de omfattande skadorna på el- och telesystemet upprätthålla fungerande telekommunikationer för 98 procent av sina kunder under hela isstormen

Krishanteringen inom telekommunikationssystemen krävde mycket omfattande insatser av ett stort antal aktörer. Exempelvis delades tusentals mobila radioenheter ut och ett stort antal reservkraftsaggregat lånades ut till telekommunikationsföretagen. Även logistiken som krävdes för att lösa problem kring driften av telenäten förutsatte omfattande och koordinerade insatser. För att kunna genomföra det stora antalet tekniska åtgärder som krävdes så var de goda relationerna mellan myndigheter och telekommunikationsindustrin, samarbetet mellan dessa och vissa gemensamma överenskommelser avgörande för att förhindra ett fullständigt sammanbrott av telekommunikationerna under isstormen.

Den centrala federala myndigheten som var engagerad i ledningen av krishanteringen inom telesektorn drog flera lärdomar av isstormen. En viktig erfarenhet var hur betydelsefull olika nationella och regionala samarbetsorgan varit för att träffa överenskommelser om krishantering. Man betonade även vikten av att organisationer på olika nivåer har kännedom om varandras situation och att lägesrapporter utbytes mellan de olika nivåerna.

En annan viktig erfarenhet var att katastrofpersonal i en krissituation har behov av att kunna koppla om sina tjänstetelefoner, även från andra platser än den ordinarie arbetsplatsen. Just förmågan att flexibelt kunna utnyttja telenätet kan ha en stor betydelse för hanteringen av en kris och dess konsekvenser.

De moderna telekommunikationernas möjligheter att styra om kommunikation på ett flexibelt sätt visade sig vara betydelsefullt för krishanteringen i samband med elavbrotten i Auckland, Nya Zeeland, i början av 1998. Elkrisen som drabbade Aucklands centrala affärsdistrikt (CBD, Central Business District) orsakades av en serie kabelbrott under januari till februari månad 1998 och kulminerade den 20 februari. Den elkris som inleddes varade i över fem veckor och störningarna i elförsörjningen kvarstod ända in i maj månad.

Auckland CBD utgörs av ett antal gatukvarter motsvarande ungefär tre kvadratkilometer och har en bofast befolkning på ca 5 000 personer. Näringslivet i CBD och de angränsande delarna av Auckland som drabbades av elavbrotten omfattar drygt 8 500 företag, vilka sysselsätter uppskattningsvis 66 000 personer. De flesta av dessa arbetspendlade dagligen från övriga Auckland-regionen. En stor del av näringslivet inom CBD kan karaktäriseras som kontorsverksamhet. Några av företagen är stora bolag med verksamhet i hela Nya Zeeland men ett betydande antal utgörs av småföretag av olika typer. Många av de mindre företagens verksamhet återfinns inom livsmedels- och restaurangsektorn och varierar storleksmässigt från små kiosker för snabbmat och vanliga restauranger till stormarknader.

Telekommunikationerna påverkades redan i ett tidigt skede av störningarna i elförsörjningen. Mot bakgrund av en tidig begäran från det drabbade elföretaget använde flera av teleoperatörerna sina reservkraftsgeneratorer redan före den 20 februari. Eftersom de viktigaste telestationerna hade tillräckligt med reservkraft så drabbades dessa stationer inte av några störningar till följd av elavbrotten. I vissa fall hade man nyligen genomfört en betydande förbättring av sin reservkraftskapacitet. Vid de mindre basstationerna i mobiltelefoninäten, som inte var utrustade med generatorer, fick man snabbt komplettera med reservkraftsförsörjning. På grund av elavbrotten uppstod det störningar i abonnentväxlar eftersom de i varierande grad var utrustade med reservkraftsförsörjning.

För att hantera elkrisen skaffade många företag reservkraftsgeneratorer för att, åtminstone delvis, få elström till sina lokaler. Man flyttade även verksamhet till lokaler utanför det drabbade området och man uppmuntrade personal att arbeta hemifrån. Möjligheterna för

olika företag att fortsätta att bedriva sin verksamhet i normal omfattning varierade beroende på vilken bransch man tillhörde. De som uppvisade störst flexibilitet var den finansiella sektorn och annan verksamhet inom tjänstesektorn, till exempel advokat- och mäklarbyråer.

De elektroniska kommunikationernas flexibilitet var betydelsefulla och ibland helt avgörande för många verksamheters möjlighet att omlokalisera. Möjligheten att automatiskt koppla vidare telefoner, faxar etc. till nya lokaler gjorde att verksamheter relativt enkelt kunde flyttas och att störningarna kunde begränsas. I en del fall kunde anställda arbeta hemifrån via modemuppkopplingar. Genom de åtgärder man vidtog kunde man bland annat bibehålla den interna kommunikationen inom organisationen och dessutom upprätthålla kontakten med kunder. Här kan man således se ett exempel på att elektroniska kommunikationer och annan informationsteknik är viktiga verktyg för att begränsa effekterna av en kris.

### 4.2.2 Samhällsviktiga funktioner

I det nedanstående presenteras samhällsfunktioner som måste fungera och vilkas betydelse förstärks i samband med svåra påfrestningar, höjd beredskap eller krig. Detta eftersom man då kan räkna med omfattande skador på människor och materiel.

Nedanstående information gällande SOS Alarm, räddningstjänsten, kommunal ledning och polisen baseras till stor del på information från en FOA-studie utförd 1999. Utvecklingen på elektroniska kommunikationsområdet går fort och det är inte omöjligt att vissa system bytts ut eller förändrats.

#### 4.2.2.1 SOS Alarm

SOS Alarm har 20 stycken SOS-centraler i Sverige. Dessa är helt beroende av fungerande telekommunikationer för att ta emot inkommande larm framför allt från 112 och i form av automatlarm. Utgående samtal går huvudsakligen till räddningstjänst, ambulanssjukvård och polis. Utalarmering sker i mycket stor utsträckning med tal, man använder då både radiokommunikation och vanlig telefoni. Datakommunikation används som komplement för att snabba upp hanteringen, då i form av Mobitex för till exempel körorder.

#### 4.2.2.2 Räddningstjänsten

Den kommunala räddningstjänsten är starkt beroende av tele- och radiokommunikation för sin verksamhet, inkommande larm vidarebefordras från SOS Alarm till brandstationen med telefon, radio eller Mobitex. Utalarmering av brandmän sker via personmottagare på 79 MHz-bandet, man använder även Minicall. I räddningstjänstbilarna finns GSM och radio.

#### 4.2.2.3 Ledning

Kommuner och länsstyrelser är ansvariga för att samordna och koordinera insatser vid större kriser. Det är därför mycket viktigt att de har fungerande system för elektronisk kommunikation för att klara denna uppgift.

För sin dagliga verksamhet använder kommunerna redan idag i stor utsträckning GSM exempelvis för samordning av arbetet inom hemsjukvård, socialtjänst och gatukontor. Man har vanligen även tillgång till räddningstjänstens radio.

Det finns en viss osäkerhet i vilken utsträckning kommunerna har redundans i sina teleförbindelser. Genom att en kommun anlitar flera teleoperatörer kan man i viss utsträckning få ökad redundans.

#### 4.2.2.4 Polisen

Polisen har mycket stort behov av tele- och radiokommunikation för den dagliga verksamheten. Inkommande larm kommer normalt till polisen via polisens telefonväxel eller direkt via SOS-centralen genom att SOS-operatör vidarekopplar samtal från 112.

Fungerande talkommunikation bedöms som det allra viktigaste för polisarbetet. Förmedling av uppdrag, information från kommunikationscentraler och kommunikation mellan patruller sker huvudsakligen med radio. Man använder även mobiltelefon i stor utsträckning för fall som inte är akuta. En annan orsak till att man använder GSM är att denna trafik inte kan avlyssnas.

Man blir allt mer beroende av datakommunikation. Det finns ett gemensamt landstäckande datanät. Nätet används för att kontakta centrala system och register. Exempel på information som kommuniceras är personuppgifter, spaningsdata och fordonsinformation.

Elavbrott på ett cirka ett dygn skall inte påverka polisens förmåga att bedriva sin verksamhet.[23]

#### 4.2.2.5 Sjukvård

Den akuta sjukvården är helt beroende av att SOS Alarm fungerar. Detta innebär mottagning av larm via 112, utlarmning av sjuktransportfordon och dirigering av dessa till skadeplatsen.

Det finns även ett stort teleberoende i materialhanteringen eftersom sjukhusens lager för vissa produkter har en marginal på några timmar.

Man är även beroende av datakommunikation. Centrala datatjänster för remisshantering, provsvar, patientadministration och liknande finns inom landstingen. Trenden går tydligt mot ett allt större beroende av elektronisk kommunikation.

#### 4.2.2.6 Elförsörjningen

Beroendet av en fungerande elförsörjning är mycket omfattande i alla samhällsfunktioner, vare sig det är fred, svår påfrestning, höjd beredskap eller krig.

Under normal drift används tele- och datakommunikationer för drift och övervakning av elnät och elproduktionsanläggningar. Elföretag har ofta egna drifttelenät men använder även de publika tele- och datanäten.

I samband med underhåll och reparationer av elnätet är beroendet av mobil telekommunikation och då framför allt talkommunikation mycket stort. Vid elavbrott dirigeras reparationspersonal från driftcentraler och utan en fungerande kommunikation dem emellan blir reparationstiden orimligt lång. Elsäkerheten för reparationspersonal blir dessutom försämrad. Svenska Kraftnät som äger och driver stamnätet för elkraft i Sverige har inte tillgång till något eget mobilradiosystem. All kommunikation mellan driftcentraler och underhållsentreprenörer i fält sker därför uteslutande med hjälp av mobiltelefon.[24]

I krissituationer ökar användandet av mobiltelefoner. Ett stort problem är att ett elavbrott minskar kapaciteten i mobilnäten allteftersom batterierna i basstationerna laddas ur, normalt brukar man dock kunna behålla täckningen. Vid en krissituation i kombination med ett elavbrott är det därför viktigt att snabbt få igång elförsörjningen till telesystemet. I

[23] Melin L. och Persson K., Polisens ledningsförmåga på regional nivå i NBC-miljö, FOA-RH-99-00425-865-SE, April 1999

[24] Beroenden mellan el- och telesystem vid omfattande och långa elavbrott, Svenska Kraftnät, 25 oktober 2001

dagsläget finns det dock ingen möjlighet att prioritera telefonsamtal för exempelvis reparationspersonal. Försök med denna typ av prioritering har dock utförts i PTS regi.

Omvänt så finns det heller idag ingen möjlighet att prioritera el till telenätet om detta behov skulle uppstå.

# 5 Samlad bedömning av hot, sårbarhet och risker för samhället

I det följande söker vi göra en samlad värdering av tänkbara hot mot de elektroniska kommunikationerna, kommunikationssystemens tekniska sårbarhet och bedömda risker för samhället om kommunikationerna inte skulle fungera. De bedömningar vi gör grundar sig på statsmakternas aktuella hotbedömningar, genomgångar av systemens principiella uppbyggnad och sårbarhet såsom redovisats i det föregående samt bedömningar av samhällets behov av att ha tillgång till säkra kommunikationer inom olika områden vid svåra påfrestningar på samhället i fred och vid höjd beredskap och krig.

## *5.1 En översyn av säkerheten behövs*

En allmän iakttagelse som vi gör är att de svenska systemen för telekommunikationer under lång tid byggts upp för att kunna fungera i rimlig utsträckning också vid höjd beredskap och i krig. Det innebär bl.a. att relativt stora satsningar gjorts för att skapa ett gott skydd mot vapenverkan för centrala delar av näten och att reservfunktioner förberetts. Nu har emellertid hotbilden förskjutits från ett militärt angrepp syftande till invasion som det dominerande fallet. I stället kommer mer begränsade militära angrepp och inte minst olika typer av svåra fredstida hot i fokus.

Det senaste decenniets avreglering och kommersialisering av telemarknaden i kombination med den snabba utvecklingen av mobil telefoni och datakommunikation har också förändrat behovet av säkra kommunikationer och möjligheterna att tillgodose det. Många verksamhetsområden i samhället har utnyttjat de vidgade möjligheter till elektronisk kommunikation som erbjuds men har också i långt högre grad än tidigare gjort sig beroende av att ständigt, snabbt och säkert kunna överföra stora informationsmängder. De värden som kommunikationsmedlen förmedlar har blivit mycket stora.

Trots traditionen att säkra kommunikationerna och arvet från tidigare utbyggt skydd finns det därför anledning att kritiskt pröva säkerheten i dagens system för elektronisk kommunikation och vad vi bygger för framtiden. De kraftigt utbyggda och avancerade system vi nu håller på att få behöver tillgodose de krav på säker kommunikation som vårt nya IT-samhälle måste ställa inför de olika typer av tänkbara hot och påfrestningar som nu ter sig aktuella.

## *5.2 Vardagens hot och risker måste alla beakta*

Den rent tekniska sårbarheten hos systemen för elektronisk kommunikation är i allmänhet ganska stor ute hos den enskilda abonnenten och i accessnäten. Här finns också inte helt försumbara vardagliga hot mot den enskilde abonnenten i form av dåligt väder, inbrott, skadegörelse, tekniska fel, olyckor som skadar kommunikationerna etc. Konsekvenserna av sådana störningar kan emellertid i allmänhet inte bedömas innebära svåra påfrestningar på samhället. Trots att de enskilda abonnenternas terminaler och accessvägar är tekniskt sårbara kan dock därför riskerna för samhället totalt sett bedömas som små.

Det hindrar inte att den enskilde abonnenten kan lida allvarlig skada av avbräck i sina möjligheter att kommunicera. De flesta företag är idag så beroende av såväl intern som extern elektronisk kommunikation att avbrott skulle medföra stora konsekvenser för verksamheten. Det är i första hand den enskildes sak att gardera sig för de risker som föreligger. Det kan göras genom att i avtal med operatörer ställa krav på tillgänglighet och ersättning vid brister, genom att undvika att göra sig beroende av ständigt fungerande

telekommunikationer, genom att anskaffa reservalternativ, genom att anskaffa lokalt skydd mot såväl dataintrång som fysiskt intrång, genom försäkringslösningar etc.

Enligt propositionen om samhällets säkerhet och beredskap bör samhällets grundläggande säkerhet och beredskap, den s.k. basförmågan, finansieras av den verksamhetsansvarige. Basförmågan avser primärt normala fredstida störningar och olyckor.[25] Enligt utredningen om elektronisk kommunikation bör driftsäkerhet under normala förhållanden vara en fråga som överlämnas till marknaden. Det är således knappast samhällets sak att ingripa i enskilda kunders eller leverantörers val av säkerhetsnivå för den elektroniska kommunikation de köper eller levererar eller att garantera säkerheten mot normalt förekommande störningar.

Samhällets ansvar ligger i stället på den övergripande nivån att skapa sådana villkor att konkurrens och marknadsmekanismer kan fungera. Det kan också vara samhällets ansvar att för att stimulera en väl fungerande marknad tillhandahålla information om hot och risker som finns och om alla verksamhetsansvarigas ansvar att själva ta hänsyn till dem. Samhället kan naturligtvis därutöver i specifika fall ingripa för att öka säkerheten i de elektroniska kommunikationerna. Det kan ske med utgångspunkt i de övriga mål (nivå 3) som anges i den i avsnitt 1.4 citerade politiska målsättning som föreslås av Utredningen om elektronisk kommunikation. Ett sådant mål är att säkerställa uthållighet och tillgänglighet under svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Genom att alla verksamheter som är beroende av elektronisk kommunikation tar ansvar för sin egen vardagssäkerhet skapas en basförmåga och en grundläggande robusthet och beredskap att motstå hot och hantera störningar. Denna basförmåga utgör en nödvändig grund och förutsättning för att samhället skall ha tillfredsställande elektroniska kommunikationer också vid svåra påfrestningar i fred och vid höjd beredskap och krig. Den tekniska infrastrukturens säkerhet måste som påpekas i den ovan nämnda propositionen om samhällets säkerhet och beredskap byggas underifrån. Det är dock inte säkert att de lokala abonnenterna alltid är medvetna om de risker som finns eller om vilka åtgärder de själva kan vidta för att öka säkerheten. Basförmågan skulle antagligen kunna förbättras om hot, risker och möjligheter att förbättra säkerheten blev mer allmänt uppmärksammade.

## *5.3 Samhällsviktiga verksamheter kräver särskilt skydd*

Det finns många samhällsviktiga funktioner som är starkt beroende av att ha tillgång till säker elektronisk kommunikation. För dessa funktioner kan redan ett lokalt bortfall av kommunikationerna medföra svåra påfrestningar på samhället. Det gäller t.ex. alarmcentraler, ledningscentraler för polis, räddningstjänst och andra s.k. blåljus-myndigheter, sjukvårdens informationssystem och driftledning för teknisk infrastruktur.

Det måste i enlighet med principerna i den nämnda propositionen om samhällets säkerhet och beredskap ställas ett grundläggande krav på dessa funktioner att inom ramen för sin ordinarie verksamhet vidta åtgärder för att skapa god säkerhet i de elektroniska kommunikationerna redan vid normalt förekommande störningar. Det kan ofta ske med enkla medel genom att t.ex. ha lokal reservkraft, anlita flera operatörer, använda flera fysiskt skilda anslutningar till telenäten och att skapa lokala skydd mot dataintrång och fysiska intrång. Den allmänna bild vi fått av vardagssäkerheten inom dessa samhällsviktiga områden är inte odelat positiv. Problem med bl.a. ansvarsfördelning och finansiering och kanske också dålig medvetenhet om sårbarhet och risker gör att brister i säkerheten finns.

[25] Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap, avsnitt 4.5

Den segdragna frågan om ett nytt gemensamt radiosystem till de s.k. blåljusmyndigheterna utgör ett exempel på detta.

## 5.4 Flera samtidiga störningar i näten svåra att bemästra

Vår bedömning är att den basförmåga av säker elektronisk kommunikation som finns i samhället och som främst drivs fram av marknadskrafterna totalt sett tillgodoser ganska höga krav på säkerhet för samhällets funktion vid enskilda störningar under normala förhållanden. Enstaka fel och enstaka avbrott ute i nätet kan i regel mycket snabbt och effektivt hanteras med omkopplingar, reservsystem etc. så att endast ett fåtal abonnenter drabbas.

Vad som kan ge större problem för de elektroniska kommunikationerna och för samhällets funktion är när flera störningar inträffar samtidigt. Det kan t.ex. ske vid väderstörningar i större områden, när någon annan större påfrestning som ett längre elavbrott eller stor olycka slår ut elektroniska kommunikationer med förvärrade svårigheter som följd eller när någon avsiktlig aktör samtidigt påverkar flera funktioner så att redundansen reduceras och reservmöjligheter försvinner.

Den ökande konvergensen mellan olika typer av elektronisk kommunikation och centraliseringen av styrfunktioner gör att även enstaka störningar i och sabotageinsatser mot systemens centrala delar kan få störningar inom en mängd delområden som följd.

Vi anser därför att de elektroniska kommunikationernas sårbarhet och risker för samhället vid svåra påfrestningar i fred och vid höjd beredskap och krig framför allt sammanhänger med möjligheten av samtidiga bortfall av flera funktioner. Det är något som föga beaktas vid den på kommersiella grunder gjorda uppbyggnaden av systemen. Sannolikheten är mycket liten att två av varandra oberoende störningar skall inträffa samtidigt och såväl abonnenter som operatörer tenderar därför att bortse från de risker som sådana sällsynta och extrema situationer skulle kunna innebära.

De begränsade intervjuer med operatörer och genomgångar av tillgängligt skriftligt material om näten som vi hittills medhunnit indikerar att det fysiska skyddet för centrala noder i stamnätet och centrala styrnoder för både fast och mobil telefoni är gott. Mer tveksamt är om skyddet mot informationsintrång är lika gott och kommer att förbli det när integrationen av fast tele, mobil tele och datatrafik ökar och informationsvägarna blir alltmer komplexa. Vi noterar dock att avsevärda försiktighetsåtgärder företas för att förhindra intrång i styrnäten.

På medelhög nivå i näten är det fysiska skyddet mindre utbyggt även om noder i regel finns i utrymmen med tillträdesskydd. Stamnätets kablar är förhållandevis oskyddade även om de är nedgrävda. När antalet fysiskt åtskilda vägar för informationsflödet är litet, som till Norrland och till Gotland, kan en sabotör som lyckas lokalisera kablarna relativt enkelt åstadkomma totala avbrott i förbindelserna. Känsligheten för långa elavbrott är också stor genom att befintlig reservkraft ofta har begränsad uthållighet.

En faktor som bidrar till ökad säkerhet är att det numera finns ganska många operatörer. Med fast abonnemang, några mobilabonnemang och bredbandsanslutning för data kan den enskilde abonnenten skaffa sig flera möjliga accesspunkter och nå en god robusthet mot många typer av störningar. Samtidigt finns risken att flera förbindelser i något led är beroende av en och samma del av transportnätet eller av någon central styrfunktion.

Kommunikationer som bygger på radioförbindelser ger i regel stor flexibilitet och visst oberoende av lokala skador vilket kan vara en fördel i extrema situationer. Basstationer och antenner kan vara känsliga för sabotage och en mer kvalificerad angripare kan bedömas kunna begränsa kontaktmöjligheterna genom radiostörning. Det kan finnas skäl att pröva

om det går att finna möjligheter att i utsatta områden förstärka de mobila kommunikationernas uthållighet, tillgänglighet och säkerhet om de skulle utsättas för kvalificerade sabotage.

## 5.5 Den inre säkerheten allt viktigare

Den tekniska utvecklingen med en mångfald av nätstrukturer, integration mellan olika typer av elektronisk kommunikation, centralisering av styrfunktioner och ökad intelligens i systemen gör att den som vill påverka de elektroniska kommunikationernas funktion måste ha en mycket ingående kännedom om systemens uppbyggnad. Det gäller såväl vid utbyggnad och drift som för den som vill sabotera kommunikationerna.

Det gör att den inre säkerheten hos olika operatörer men också hos användarna av elektronisk kommunikation får allt större betydelse. En person som arbetar hos en operatör kan få kännedom om systemuppbyggnad och få både datatillgång och fysiskt tillträde till känsliga delar av systemens mjuk- och hårdvara. Personen skulle kunna åstadkomma stor skada genom att utnyttja sin kunskap och sina möjligheter att påverka för att skada de elektroniska kommunikationerna. En sådan insider kan själv tänkas vilja av någon anledning skada samhället eller värvas som sabotör av en grupp av brottslingar eller terrorister eller av en annan stat som vill göra detta. Tillgång till insiderkunskap är viktig också för den yttre sabotör som vill orsaka störningar genom att klippa av kablar eller förstöra knutpunkter. Utan att känna till vilka alternativa vägar som finns eller vilken funktion som olika nätelement har är det svårt att allvarligt skada de elektroniska kommunikationerna.

En viktig aspekt av säkerhetsarbetet inom alla verksamheter som utnyttjar eller tillhandahåller elektronisk kommunikation bör därför vara att begränsa möjligheterna till insyn och påverkan från egen personal, inhyrda entreprenörer eller samverkande parter. Det kan göras genom gradering av behörighet, identitetskontroll, tillträdesskydd till lokaler, inloggning, skyddade terminaler, begränsad spridning av känslig information, personkontroll etc. Särskilt viktig är den inre säkerheten när det gäller systemuppbyggnad, stamnät och styrfunktioner. Dessa områden är med dagens säkerhetspolitiska hotbild närmast jämförbara med känsliga punkter i det gamla invasionsförsvaret.

## 5.6 Det ömsesidiga beroendet mellan el och tele utgör ett påtagligt riskområde

All elektronisk kommunikation är beroende av elförsörjning i varje fall inom näten och utom för fast telefoni också separat vid terminaler. Mobiltelefoner har dock relativt lång drifttid på egna batterier och kan lätt laddas också via billaddare. Utom längst ut i näten finns reserver i form av batterier eller reservkraftverk. Abonnenter med avbrottskänslig verksamhet har ofta egen reservförsörjning med el. Uthålligheten för reservförsörjningen är dock begränsad. När ett elavbrott sker är fungerande elektroniska kommunikationer ofta viktiga för att snabbt kunna lokalisera och avhjälpa fel. Särskilt viktiga är mobila telesystem.

Långvariga och omfattande elavbrott är mycket sällsynta, men om de inträffar får de mycket omfattande konsekvenser för många funktioner i samhället, inte bara telekommunikationerna. Därmed utsätts samhället för stora påfrestningar och behovet av elektronisk kommunikation för att hantera situationen blir starkt. Den alltmer ökande centraliseringen av styrningen av kommunikationsflödet medför att mer långvariga elavbrott på olyckliga punkter t.ex. i viktiga delar av stamnätet kan få mycket vittgående

verkningar både geografiskt och när det gäller de verksamheter som påverkas. Just därför är ofta reservkraften särskilt väl tillgodosedd på dessa punkter.

Något som utgör ett påtagligt riskområde i händelse av flera samtidiga störningar är detta ömsesidiga beroende mellan systemen för elförsörjning och elektronisk kommunikation. Väderstörningar drabbar ofta samtidigt både elförsörjning och telekommunikationer och kan få en varaktighet som gör batterireserver otillräckliga. De samlade systemen för elförsörjning och elektronisk kommunikation kan även bedömas utgöra intressanta mål för terrorister, sabotörer eller militära insatser mot mål i Sverige. Även om de mest centrala noderna är skyddade finns många möjligheter till påverkan med relativt enkla medel för den som har tillräcklig kännedom om systemens uppbyggnad. De reserver som finns är knappast dimensionerade för sådana extrema situationer. Sabotage som omfattar även reservkraften kan bli mycket verkningsfulla.

## 5.7 Tillförlitlighet en ny dimension av sårbarhet och risker

De informationstekniska hoten har tillfört en ny dimension till de elektroniska kommunikationernas sårbarhet och därmed förknippade risker. Det handlar inte längre bara om att ha tillgång till en förbindelse med tillräcklig kapacitet utan också om att kunna lita på riktigheten såväl av den uppkopplade förbindelsen som av den information som överförs. Det gör det nödvändigt att beakta inte bara kommunikationernas uthållighet och tillgänglighet utan också deras tillförlitlighet. På denna punkt behöver enligt vår mening den ovan citerade målsättning kompletteras som föreslagits av Utredningen om elektronisk kommunikation (jämför avsnitt 1.4).

Vår bedömning är att medvetenheten om problemen med tillförlitlighet finns när det gäller datakommunikation och Internet, i varje fall hos användare som hanterar stora värden och viktiga verksamheter. Vi är dock inte övertygade om att de säkerhetsinsatser som görs räcker för att möta systematiska och litet mer avancerade informationstekniska angrepp mot de elektroniska kommunikationerna. Vi befarar att sådana angrepp skulle kunna åstadkomma avsevärda störningar i samhället och beröra alla typer av elektronisk kommunikation. De åtgärder som vidtas för att allmänt öka IT-säkerheten i samhället har stor relevans också för de elektroniska kommunikationernas tillförlitlighet.

Vi bedömer att det i framtiden måste bli ett ökande ansvar för operatörer att medverka till god tillförlitlighet i den information som man förmedlar. Det gäller naturligtvis särskilt Internet-operatörer men kan med den ökande konvergensen beröra alla typer av elektronisk kommunikation. Mycket av detta måste vara resultatet av fredstida kommersiella åtaganden men det bör också vara ett samhällsansvar att tillse att tillförlitligheten kan bestå vid svåra påfrestningar på samhället i fred och vid höjd beredskap och krig.

## 5.8 Säkerheten ett internationellt problem

De elektroniska kommunikationerna har kommit att bli alltmer gränsöverskridande till sin karaktär. Informationen sänds i ökande utsträckning längs vägar som också går utanför landets gränser även vid förbindelse mellan två inhemska punkter. Många operatörer är gränsöverskridande. Det är inte omöjligt att det kommer att uppstå en situation där operatörer vill förlägga styrning av kommunikationerna och nödvändiga databaser utanför landets gränser. Omvänt finns redan idag styrorgan i Sverige för andra länder.

Säkerheten i datakommunikationer är sedan länge ett utpräglat internationellt problem. Meddelanden med illasinnad kod eller överbelastningsattacker kan t.ex. komma från andra länder och nöjligheten att skydda sig beror bl.a. på vilka möjligheter som finns där att spåra sådana meddelanden. Åtgärder för att motverka informationstekniska hot drivs

framför allt genom internationellt verksamma företag och utvecklingen av internationella normer.

Elektronisk kommunikation i Sverige blir därmed beroende av hur väl kommunikationssystemen skyddas och fungerar i andra länder. Det omfattande internationella samarbete under normala förhållanden som snabbt växer fram mellan såväl operatörer som reglerande myndigheter måste utgöra grunden för att skapa tillgängliga och säkra elektroniska kommunikationer. Även om vi söker finna inhemska lösningar för säkerhet i elektroniska kommunikationer vid svåra påfrestningar på samhället i fred, höjd beredskap och krig, kommer säkerheten också att vara beroende av ett internationellt samarbete.

Samtidigt är det värt att påpeka att internationaliseringen även kan tänkas fungera som en återhållande faktor för en angripare om han riskerar att dra på sig även andra nationers vrede.

## 5.9 Ljudradio och TV måste ingå i en helhetsbild

I detta arbete behandlas en mängd system för elektronisk kommunikation och vi har inte begränsat oss till sådana system för vilka PTS har ett utpekat ansvar. Vi har under arbetets gång funnit att det finns anledning att vid en genomgång av sårbarheten i systemen för elektronisk kommunikation och risker för samhället också ta med distribution av ljudradio och TV i bilden. Redan idag är radio och i begränsad utsträckning TV tillgängliga över Internet. Olika former av interaktiv kommunikation över kabel-TV nät börjar utvecklas. Formerna för informationsspridning och kommunikation blir alltmer integrerade. Vid svåra påfrestningar i fred och vid höjd beredskap och krig spelar tillgång till snabb och tillförlitlig information från media en stor roll. Vi uteslöt dock från början distribution av ljudradio och TV från vår analys och har inte haft tillfälle att utöka den till att omfatta också dessa områden.

# 6 Fortsatt arbete med utformning av en strategi

Det fortsatta utredningsarbetet skall leda fram till en strategi för att öka motståndskraften hos telekommunikationerna så att de blir uthålliga, tillgängliga och tillförlitliga under svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Man kan diskutera vad en strategi för åtgärder bör omfatta. I varje fall bör den omfatta en allmän och långsiktig målformulering, vad man långsiktigt syftar till att uppnå med åtgärderna. Där kan förslaget från Utredningen om elektronisk kommunikation utgöra en grund med det tillägg om tillförlitlighet som diskuterats i avsnitt 5.7.

Utöver en allmän målsättning bör en strategi för arbetet med åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och med att öka beredskapen inför höjd beredskap och krig omfatta principer för hur prioriteringar bör göras mellan olika delområden och på vilket sätt satsningar bör göras för att stärka säkerheten. Uppdraget talar om en strategi för en treårsperiod vilket indikerar att regeringen möjligen också väntar sig att strategin skall omfatta en översiktlig plan för de åtgärder som bör genomföras under perioden.

Den fortsatta utredningen behöver utöver att värdera olika typer av åtgärder också fördjupa och komplettera analysen av risk och sårbarhet, t.ex. beträffande ljudradio och TV.

En grundläggande indelning av de åtgärder som diskuteras kan vara sådana som syftar till att förebygga att störningar uppstår och sådana som syftar till att kunna lindra verkningar om störningar trots allt skulle uppstå. Bland förebyggande åtgärder kan det bl.a. vara aktuellt att överväga

- att granska de elektroniska kommunikationernas säkerhet hos samhällsviktig verksamhet,
- att bidra till att förbättra skyddet för kritiska delar av infrastrukturen mot både fysiska och elektroniska hot framför allt i samband med utbyggnad,
- att öka nätverkens flexibilitet och redundans genom att t.ex. tillföra nya maskor i nätet,
- att bidra till ökad effektivitet och säkerhet i styrning och underhåll av näten,
- att stödja satsningar på inre säkerhet för vitala delar av organisationer och system för elektronisk kommunikation,
- att utveckla samarbetet om säkerhet mellan staten och operatörer inom teknisk infrastruktur främst el- och teleområdena,
- att förbättra metoder och samarbetsformer för att skydda elektroniska kommunikationer mot informationsintrång,
- att utveckla det internationella samarbetet för säkerhet.

Bland åtgärder för att kunna lindra verkningar vid svåra påfrestningar i fred, höjd beredskap och krig kan det bl.a. vara aktuellt att överväga

- att öva krishantering inom den tekniska infrastrukturen i första hand el- och telesystemen,
- att utveckla organisatoriska och tekniska möjligheter för omkoppling i kris-situationer mellan olika operatörers nät,

- att anskaffa reservutrustningar och mobila system som kan sättas in för att hantera svåra störningar,
- att tillgodose behovet av personal i kriser med hjälp av förberedd reservpersonal,
- att stärka möjligheterna till flexibel omlokalisering av trafik till nya terminal-anknytningar.

Som grund för att välja och utforma åtgärder för att höja säkerheten bör det dessutom övervägas att ge PTS till uppgift

- att systematiskt och fortlöpande insamla och analysera information om elektronisk kommunikation i samhället, hur systemen är uppbyggda och utvecklas, hur utnyttjande och flöden förändras och hur säkerheten tillgodoses,
- att regelbundet och vid behov genomföra praktiska tester av de elektroniska kommunikationernas uthållighet, tillgänglighet och tillförlitlighet.

En principiell fråga att diskutera kan vara i vilken utsträckning som staten bör söka påverka enskilda aktörers säkerhetsrelaterade agerande och i vilken utsträckning som man i stället bör låta marknaden utvecklas och vid behov i efterhand gå in med kompletterande säkerhetsåtgärder. Den traditionella formen inom civilt försvar har snarast varit den senare. Det starka sambandet mellan vardagssäkerhet och säkerhet vid svåra påfrestningar samt höjd beredskap och krig gör dock tillsammans med den snabba utvecklingen på området att mycket talar för ett nära och löpande samarbete mellan staten och enskilda inom området. Staten kan påverka de enskilda aktörerna genom lagstiftning, ekonomiska incitament, information och ömsesidiga överenskommelser till gemensam nytta.

Sedan 1997 sker en samlad planering av statens åtgärder för att för att höja teleberedskapen mot allvarliga fredstida hot och påfrestningar och för att tillgodose totalförsvarets behov vid höjd beredskap och krig. Insatserna finansieras till cirka hälften genom avgifter från teleoperatörerna. Avgifterna tas ut för åtgärder som skall ge det fasta allmänna telenätet tillräcklig robusthet och flexibilitet mot fredstida hot och påfrestningar och som är till nytta för operatörerna i fredstid. Hittills har avgiften endast erlagts av Telia AB men regeringen avser att se över grunden för avgiftsuttaget i syfte att ge den en mer konkurrensneutral utformning.[26] Regelverket för hur avgifterna tas ut och utnyttjas behöver ses över så att de rimmar med de målsättningar som Utredningen om elektronisk kommunikation föreslår (jämför avsnitt 1.4).

Det fortsatta arbetet med att utforma strategin bör omfatta en värdering av vad olika typer av åtgärder betyder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och öka beredskapen inför höjd beredskap och krig. En sådan värdering måste ta hänsyn till såväl kostnader för åtgärderna som bedömd nytta av dem. Det kommer knappast att vara möjligt att göra en strikt värdering av samhällsnyttan och att finna en optimal lösning. Därför är osäkerheterna alldeles för stora och förekommande samband och möjliga hot alldeles för komplexa. Det torde mer bli fråga om att söka peka på påtagliga brister och finna rimliga lösningar för att möta dem. Det torde också i många fall snarare vara fråga om att finna processer för att fortlöpande kunna hantera säkerhetsfrågorna än att redan från början peka ut en lämplig avvägning. För detta talar bl.a. den snabba tekniska utvecklingen som kan förväntas skapa såväl nya problem som möjligheter att lösa dem.

[26] Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap, avsnitt 7.4.

# Referenser

## *Litteraturförteckning*

Billinger, Nils Gunnar, *När blir en avgrävd telekabel ett säkerhetspolitiskt problem?*, Särtryck ur Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift 2/2002

Brevad-Jensen, Göran, *Beroenden mellan el- och telesystem vid omfattande och långa elavbrott*, Svenska kraftnät, 25 oktober, 2001

Energimyndigheten, *Ny helhetssyn för elberedskap – Delrapport till regeringen*, 1 november, 2001

Fischer, Georg; Molin,Staffan, *Isstormen i Kanada*, FOI, maj 2001, FOI-R-0103-SE http://www.foi.se/raw/images/8597_Kanada1998.pdf

FOI, *Elektromagnetiska vapen och skydd,* FOI orienterar om, nummer 1, 2001

*Fortsatt förnyelse av totalförsvaret*, Proposition 2001-02:10, http://forsvar.regeringen.se/propositionermm/propositioner/pdf/p200102_10.pdf

Frost, Christina; Molin, Staffan; Pettersson, Ulf; Ånäs, Per, *Svåra påfrestningar – Säkerheten inom el, tele, rundradio vid ett nytt totalförsvarsperspektiv*, FOA, juni 1996

Glaessner, Thomas; Kellermann, Tom; McNevin, Valerie, *Electronic Security: Risk Mitigation in Financial Transactions, Public Policy Issues,* The World Bank, June 2002

*Hagen , Janne Merete; Fridheim, Håvard,* Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System, *FFI, September 1999,* http://www.isn.ethz.ch/crn/extended/workshop_zh/Norway_Tel.pdf

Jönsson, Britt-Marie, *Uppdrag till Post och telestyrelsen avseende säkerheten i telenäten vid svåra påfrestningar*, PTS, 14 mars, 2002, http://www.pts.se/dokument/getFile.asp?FileID=2278

Melin, L.; Persson, K., *Polisens ledningsförmåga på regional nivå i NBC-miljö*, FOA-RH-99-00425-865-SE, april 1999

Molin, Staffan; Fischer, Georg, *Elavbrotten i Auckland,* FOI, februari 2001, FOI-R-0102-SE http://www.foi.se/raw/images/8596_auckland1998.pdf

Näringsdepartementet, *Regleringsbrev för budgetåret 2002 avseende PTS,* 20 december, 2001

Pettersson, Ulf; Wulff, Petter; Fischer, Georg, *Sårbarhet i de civila telekommunikationerna*, FOA, oktober 1999, FOA-R-99-01221-240-SE.

*Proposition 2001-02:158,* Samhällets säkerhet och beredskap, *http://forsvar.regeringen.se/propositionermm/propositioner/pdf/p200102_158.pdf*

PTS, *Bedömning av sårbarhet i telenäten vid en svår påfrestning,* 30 november, 2001, http://www.pts.se/dokument/getFile.asp?FileID=2529

PTS, *Drift av Internet i Sverige oberoende av funktioner utomlands,* http://www.pts.se/dokument/getFile.asp?FileID=1849

PTS, *IT-infrastrukturen i Sverige – Tillgänglighet i olika delar av landet*, 16 augusti 2002, http://www.pts.se/dokument/getFile.asp?FileID=3113 http://www.pts.se/dokument/getFile.asp?FileID=3114

PTS, *IT-infrastrukturen i Sverige – Utbyggnad, tillgänglighet och måluppfyllelse*, 15 augusti, 2001,
http://www.pts.se/dokument/getFile.asp?FileID=2379
http://www.pts.se/dokument/getFile.asp?FileID=2385

PTS, *Säker elförsörjning för telefunktionen*, 29 oktober 2001, diarienummer 01-25310

Rollén, Berit, *Ett nät för trygghet - Rapport från Uppdrag Tetra radiokommunikation*, Näringsdepartementet 2002,
http://naring.regeringen.se/propositioner_mm/rapporter/uppdrag_tetra_20020327.pdf

Rafting, Anders, *Internets robusthet*, PTS, 15 december 2001,
http://www.pts.se/dokument/getFile.asp?FileID=2763

*Räty, Riitta; Christiansson, Henrik; Fischer, Georg,* Förstudie: IT-relaterade hot mot den svenska drivmedelsdistributionen, *FOI, december 2001*

Statskontoret, *Den svenska delen av Internet*, 1997:18,
http://www.snus.se/info/internetutred/
(Sammanfattning av rapporten finns i proposition 99/00:86, bilaga 2,
http://naring.regeringen.se/propositioner_mm/propositioner/pdf/it/bil02.pdf )

SOU 1998:143, *Ett tryggare Sverige. Ett gemensamt system för mobil kommunikation.*

SOU 2001:41, *Säkerhet i en ny tid,*
http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41a.pdf
http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41b.pdf
http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41c.pdf

SOU 2002:60, *Lag om elektronisk kommunikation,*
http://naring.regeringen.se/propositioner_mm/sou/pdf/sou2002_60a.pdf

Ternblad, Sten; Wulff, Petter med Andersson, Hans; Kekki, Veikko, *Jugoslavienkriget 1999. Infrastrukturen i skottlinjen*, FOI, augusti 2002, FOI-R-0544-SE

ÖCB, *Infrastrukturuppdraget – Uppdrag 9*, 15 mars, 2000,
http://www.ocb.se/dokument/filer/Infrastrukturuppdraget.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga1.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga2.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga3.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga4.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga5.pdf
http://www.ocb.se/dokument/filer/ISU_Bilaga6.pdf

Öhrlings, PriceWaterhouseCoopers, *Kartläggning av tele och IT-infrastruktur*, mars 1999,
http://www.pts.se/dokument/getFile.asp?FileID=1174
http://www.pts.se/dokument/getFile.asp?FileID=1175

## *Intervjuer*

Under arbetet genomfördes intervjuer med:

- Jan-Olof Borgén, generalmajor, konsult, juni 2002
- Alf Tengström, tidigare på PTS, september 2002
- Bo Bergner, teknisk direktör, PTS, augusti 2002

samt med representanter från:

- Telia/Skanova, augusti 2002

- Stokab, augusti 2002
- Tele2, augusti 2002
- Vodafone, september 2002