



Robusta elektroniska kommunikationer

Strategi för åren 2003-2005

Förord

Regeringen gav med regleringsbrevet för 2002 Post- och telestyrelsen (PTS) ett uppdrag att 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.

I föreliggande rapport redovisar PTS nämnda regeringsuppdrag. Arbetet med framtagningen av strategin inleddes med en genomgång av tidigare utredningar och annat bakgrundsmaterial för att bl.a. ta tillvara erfarenheter från större störningar både inom Sverige och utomlands. Därefter analyserades och strukturerades materialet för att formulera själva strategin. Faktaunderlag och synpunkter har under arbetets gång inhämtas från myndigheter, länsstyrelser, kommuner och telekomoperatörer samt nätägare.

Strategin har tagits fram av Jonny Nilsson och Eva Ekenberg, PTS. Konsulter från BDO Consulting Group Stockholm AB och Totalförsvarets forskningsinstitut har biträtt i framtagningen.

Rapporten markerar att arbetet med att skapa säkra elektroniska kommunikationer i extraordinära situationer nu går in i en ny fas.

Det omfattande beredskapsarbete som genomförts det senaste decenniet har nu i viktiga delar nått de primära mål som eftersträvades för att skydda de fasta telekommunikationerna och efterhand även de mobila mot militära angrepp och allvarliga störningar. Mycket har dock hänt som gör det nödvändigt att förnya säkerhetsarbetet och ge det en ny inriktning.

Hotbilden har förändrats. Tänkbara väpnade angrepp från någon annan stat ter sig alltmer begränsade och avlägsna. Å andra sidan har möjligheten av sabotage, terroristangrepp och stora olyckor kommit i förgrunden. Den starkt ökande användningen av olika former av elektronisk kommunikation, inte minst datakommunikation och Internets utbredning, gör samhället alltmer beroende av säkert fungerande kommunikationer. De tekniska system som används för kommunikation blir alltmer komplexa och sammanlänkade och integrerar i stor utsträckning ljud, bild och data i digital form i samma kanaler. Elberoendet är stort. Utslagning av vitala delar av kommunikationerna kan ge stora konsekvenser för samhället.

De stora förändringarna av hot, teknik och samhällets beroende gör det nödvändigt att utveckla arbetet med att skydda de elektroniska kommunikationerna. Sverige är i hög grad beroende av effektiva och säkra elektroniska kommunikationer. Tillförlitlighet, uthållighet och tillgänglighet behöver tillgodoses inte minst när samhället utsätts för svåra påfrestningar. Skyddet måste utformas så att det svarar mot dagens hot och vad vi kan förutse för framtiden, mot den snabba tekniska utvecklingen på området och mot de alltfler tjänster som är beroende av säkert fungerande kommunikationer.

Strategin som presenteras ger en ny inriktning av det arbete som PTS som ansvarig myndighet avser driva under de närmaste åren för att tillgodose behovet av tillförlitlighet, uthållighet och tillgänglighet hos de elektroniska kommunikationerna vid kriser, höjd beredskap och krig.

Nils Gunnar Billinger
Generaldirektör

Innehåll

Sammanfattning	2
Summary	4
1 Inledning	6
1.1 PTS grundläggande uppdrag	6
1.2 Regeringsuppdraget	6
1.3 Tolkning av uppdraget	6
1.4 Metod för arbetet med strategin	8
1.5 Rapportens struktur	9
2 Politiska och organisatoriska utgångspunkter.....	11
3 Skydd av de elektroniska kommunikationerna förr och nu	14
3.1 Tidigare satsningar.....	14
3.2 Dagens behov.....	14
4 Mål för skyddet av de elektroniska kommunikationerna	16
5 Principer för samarbete.....	18
6 Åtgärdsområden	20
6.1 Stimulans till ett ökat användaransvar inom elektroniska kommunikationer.....	21
6.2 Ökad redundans och flexibilitet i nätverk	24
6.3 Förbättrat skydd mot både fysiska och elektromagnetiska hot	28
6.4 Minskad känslighet för informationsoperationer samt åtgärder för att motverka sådana.....	30
6.5 Säkrare elförsörjning och fördjupat samarbete mellan el- och teleområdena.....	32
6.6 Stöd till satsningar på inre säkerhet	34
6.7 Fördjupat internationellt samarbete.....	36
6.8 Förbättrad förmåga till krishantering inom elektroniska kommunikationer	38
6.9 Granskning av vilken funktionssäkerhet som uppnås i näten	40
7 Grunder för prioritering av insatser	42
Litteratur	43

Bilagor

Bilaga 1 – Telekommunikationernas sårbarhet och risker för samhället ⁴⁴	
Bilaga 2 – Sårbarhet i distributionen av radio och TV	50

Sammanfattning

Post- och telestyrelsen (PTS) har av regeringen fått i uppdrag 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.

PTS har valt att till begreppet telekommunikationer hänföra alla typer av elektronisk kommunikation. Föreliggande dokument redovisar den strategi som PTS, inom ramen för det uppdrag som givits myndigheten i förordning, instruktion och regleringsbrev, avser tillämpa i sin myndighetsutövning och i beslut inom detta område. PTS har tolkat uppdraget, vilket överensstämmer med regeringens tolkning av begreppet i prop. 2002/03:110 sidan 339, som att den begärda strategin skall ange principer för arbetet med att minska sårbarheten och öka robustheten hos de elektroniska kommunikationerna.

En enskild åtgärd för att höja säkerheten är ofta verkningsfull vid såväl fredstida kriser som för att öka beredskapen inför höjd beredskap och krig. Därför redovisas angelägna åtgärdsområden utan en strikt uppdelning på kris, svåra påfrestningar i fred resp. höjd beredskap och krig.

PTS redovisar ett till dagens förhållanden anpassat mål för skyddet av de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig. Detta mål utgör en precisering av de mål statsmakterna fastställt för samhällets säkerhet och beredskap.

PTS redovisar principer för samarbete om säkerhet mellan företrädare för allmänna intressen och enskilda aktörer inom elektronisk kommunikation. Utgångspunkten för samarbetet skall vara de former för elektronisk kommunikation som under normala förhållanden och fri konkurrens växer fram i samhället. Samarbetet med enskilda aktörer skall syfta till att öka medvetenheten om de svåra situationernas krav och att finna lämpliga kompletterande åtgärder för att tillgodose skyddet för de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig.

Därefter redovisas ett antal olika åtgärdsområden som PTS anser angelägna för insatser. För varje sådant område redovisas syfte, inriktning och insatser.

Åtgärdsområdena är:

1. Stimulans till ett ökat användaransvar inom elektroniska kommunikationer
2. Ökad redundans och flexibilitet i nätverk
3. Förbättrat skydd mot både fysiska och elektromagnetiska hot
4. Minskad känslighet för informationsoperationer samt åtgärder för att motverka sådana
5. Säkrare elförsörjning och fördjupat samarbete mellan el- och teleområdena
6. Stöd till satsningar på inre säkerhet

7. Fördjupat internationellt samarbete
8. Förbättrad förmåga till krishantering inom elektroniska kommunikationer
9. Granskning av vilken funktionssäkerhet som uppnås i näten

Avslutningsvis redovisar PTS grunder för prioritering av insatser.

Summary

The Government has commissioned the National Post and Telecom Agency (PTS) to present for the telecommunications a strategy for the work to reduce consequences for society of severe peacetime emergencies and increase the preparedness to face a state of national alert and war. The strategy should cover the years 2003-2005.

PTS has chosen to include all forms of electronic communication in the notion of telecommunications. PTS's interpretation of the commission is that the desired strategy should define principles for the work to reduce vulnerability and increase robustness of the electronic communications.

A specific measure to increase security is often effective to reduce consequences to society of severe peacetime emergencies as well as to increase preparedness to face a state of national alert and war. Important areas in which measures should be taken are therefore presented without being classified as targeting specifically severe peacetime emergencies or a state of national alert and war.

PTS presents a goal for the protection of electronic communications during severe peacetime emergencies, a state of national alert and war. This goal is a specification made by PTS based on current general goals for society's safety and preparedness.

PTS presents principles for public/private cooperation regarding safety in electronic communications. Such cooperation should be based on the forms of electronic communication that under normal conditions and free competition evolve in society. The purpose of cooperation with individual actors should be to increase their consciousness of the demands of severe emergencies and to find suitable complementary measures to ensure the protection of electronic communications in times of severe peacetime emergencies, a state of national alert and war.

A number of areas are presented in which PTS considers it to be of special importance to take measures. For each area a purpose, a directive of the measures and examples are presented. The areas are:

1. Stimulation of an increased user responsibility concerning electronic communications
2. Increased redundancy and flexibility in networks
3. Improved protection against physical and electromagnetic threats
4. Reduced sensibility to information operations and measures to counter them
5. A more secure power supply and increased cooperation between the areas of power distribution and telecommunication
6. Support to strengthening of inner security
7. More profound international cooperation
8. Increased ability to manage crises within electronic communications

9. Review of the operational security achieved in the networks of electronic communication

PTS also presents principles for prioritization between measures.

1 Inledning

1.1 PTS grundläggande uppdrag

Post- och telestyrelsen är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom post-, tele- och radioområdena.

PTS har såsom sektorsmyndighet ett ansvar för att samhällets behov av telekommunikationer tillgodoses och ett uppdrag att vidta åtgärder för att förebygga och motverka sårbarhet inom sitt sektorsområde.

Enligt 4 § förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap skall PTS planera och vidta åtgärder för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom samverkansområde teknisk infrastruktur.

1.2 Regeringsuppdraget

Regeringen gav med regleringsbrevet för 2002 Post- och telestyrelsen (PTS) följande uppdrag:

”PTS skall 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.”

En delredovisning insändes av PTS till regeringen den 30 september 2002 (PTS diarienummer 02-12281). Med denna rapport slutredovisas uppdraget.

1.3 Tolkning av uppdraget

1.3.1 Alla typer av elektronisk kommunikation

I analogi med förslaget till ny lag om elektronisk kommunikation prop 2002/03:110 har PTS valt att till begreppet telekommunikationer hänföra alla typer av elektronisk kommunikation för att överföra och utbyta information. Överföringen kan ske med traditionell analog teknik eller med digitaliserad

teknik eller med en kombination av dessa. Den kan ske i kopparledningar och koaxialkablar, i optiska fibrer 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 olika formerna av elektronisk kommunikation i ett helhetsperspektiv.

1.3.2 Myndighetens inriktning för att tillgodose skyddet men inte en konkret plan

PTS har utformat strategin med utgångspunkt i gällande politiska inriktning och verksamhetsmässiga struktur för samhällets säkerhet och beredskap i stort. Strategin anger hur PTS som sektoransvarig myndighet avser att utöva statens roll för att tillgodose tillförlitlighet, uthållighet och tillgänglighet hos de elektroniska kommunikationerna vid svåra påfrestningar i fred, höjd beredskap och krig.

PTS tolkar uppdraget som att strategin skall ange principer för arbetet med att minska sårbarheten och öka robustheten hos de elektroniska kommunikationerna. Principerna skall tillämpas av PTS under åren 2003 – 2005. De konkreta åtgärderna däremot bör syfta till att höja säkerheten i såväl ett kortsiktigt som längre perspektiv. PTS har valt att i strategin ange ett utifrån den politiska inriktningen preciserat mål för skyddet av de elektroniska kommunikationerna samt en inriktning av på vilka sätt detta skydd bör tillgodoses. Strategin utgör dock inte en plan för vilka konkreta insatser som bör genomföras under de aktuella åren.

Sätt att nå målet beskrivs dels i generella termer dels genom en inriktning av de insatser som bör göras inom olika åtgärdsområden med förslag på insatser och grunder för prioritering. Viktiga sådana åtgärdsområden utgörs av de i uppdraget särskilt utpekade frågorna rörande säkerhetsarbetet avseende noder och redundans i IT-infrastruktur med hög överföringskapacitet (avsnitt 6.2 och 6.3) resp. samplanering mellan berörda myndigheter avseende beroenden mellan el- och telesystem vid omfattande och långa elavbrott (avsnitt 6.5).

1.3.3 Begreppen svåra påfrestningar i fred, höjd beredskap och krig

Med svåra påfrestningar på samhället i fred avses olika slag av extraordinära situationer där det uppstår allvarliga störningar i viktiga samhällsfunktioner och där det krävs att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen och därmed begränsa konsekvenserna enligt prop. 2001/02:158 sida 25. PTS bedömer att påfrestningarna kan ha sin grund i slumpmässiga faktorer som t.ex. oväder, naturkatastrofer, tekniska fel eller stora olyckor men kan också vara en följd av att någon aktör t.ex. en terrorist eller annan avancerad brottsling avsiktligt söker skada och påverka samhället.

Begreppet extraordinära händelser i fredstid används i ”Lag (2002:833) om extraordinära händelser i fredstid hos kommuner och landsting” och definierades i propositionen ”Extraordinära händelser i kommuner och landsting” (prop. 2001/02:184). Begreppet används på ett likartat men något vidare sätt än begreppet svåra påfrestningar på samhället i fred. Typiska händelser som avses är väderrelaterade händelser av större omfattning, som t.ex. större översvämningar och omfattande snöoväder. PTS utvecklar i strategin inte skillnaden mellan de båda begreppen.

Vid höjd beredskap vidtar Sverige förberedelser för att kunna möta angrepp och hot mot landets frihet och självständighet. I krig utsätts landet för väpnat angrepp från en annan stat. Den tekniska infrastrukturen utgör ett tänkbart mål för sabotörer inför ett angrepp och för direkta militära insatser under ett sådant.

1.3.4 Klassificering av risk, sårbarhet och åtgärder

Risk och sårbarhet tolkas i vid mening. Analysen av dessa områden omfattar tre steg. De utgör

1. tänkbara hot mot de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig,
2. den tekniska sårbarheten i kommunikationssystemen för dessa hot samt
3. tänkbara konsekvenser för samhället av störningar i kommunikationerna.

Hoten är till sin karaktär delvis olika i fred, höjd beredskap och krig men såväl teknisk sårbarhet som konsekvenser för samhället är likartade oberoende av om det råder fred, höjd beredskap eller krig. En och samma åtgärd för att höja säkerheten är ofta verkningsfull såväl för att minska konsekvenserna av svåra påfrestningar på samhället i fred som för att öka beredskapen inför höjd beredskap och krig. Strategin redovisar därför angelägna åtgärdsområden utan en strikt uppdelning på svåra påfrestningar i fred resp. höjd beredskap och krig. Analysen fokuserar dock på åtgärder som behövs för att komplettera den säkerhet som marknadskrafterna förväntas skapa. Det handlar då inte minst om att söka förhindra samtidiga och omfattande störningar på flera ställen och att kunna hantera sådana om de trots allt inträffar.

1.4 Metod för arbetet med strategin

Arbetet har letts från PTS, enheten för samhällsättagande. Utredningsarbetet har därutöver genomförts av Göran Franzén från BDO Consulting Group Stockholm AB och Svante Barck-Holst och George Fischer från Totalförsvarets forskningsinstitut. I utredningsarbetet har ingått en genomgång av tidigare utredningar och annat bakgrundsmaterial som bedömts ha relevans för frågeställningarna. Strävan har varit att ta tillvara empiriska erfarenheter

från inträffade störningar, exempelvis teleavbrottet i Uppsala den 2 oktober 2002, tunnelbränderna i Kista 2001 och 2002, isstormen i Kanada 1998 och elavbrottet i Auckland samma år. Arbetet med att strukturera och analysera materialet och att formulera slutsatser har genomförts i flera varv.

Arbetet med strategin har redovisats inom Samverkansområdet teknisk infrastruktur. Ingående myndigheter i samverkansområdet inklusive Styrelsen för psykologiskt försvar liksom Försvarsmakten har givits tillfälle att lämna synpunkter på utkast. Inkomna synpunkter har i allt väsentligt beaktats.

Sakunderlag och synpunkter har vidare inhämtats från ett antal telekommunikations- och nätoperatörer; RegNet i Gästrikland, Stokab AB, Tele2 AB, TeliaSonera AB, Teracom AB och Vodafone AB. Synpunkter har också inhämtats från länsstyrelserna i Uppsala län, och Västerbottens län samt Sotenäs och Tanums kommuner. Sakunderlaget har utnyttjats under arbetets gång och inkomna synpunkter på utkast har i allt väsentligt beaktats.

1.5 Rapportens struktur

Rapporten är strukturerad med inledning och bakgrund i kapitel 1, 2 och 3, därefter följer den framtagna strategin i kapitel 4 till och med 7.

I **kapitel 2** redovisas de allmänna politiska och organisatoriska utgångspunkter för samhällets säkerhet och beredskap som utgör grunden för statens arbete med att minska sårbarheten och höja robustheten för de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig. Denna text finns med framför allt för att ge dem som skall tillämpa strategin för skyddet av de elektroniska kommunikationerna en lättillgänglig bakgrund om hur samhällets beredskap och säkerhet hanteras i stort.

I **kapitel 3** redovisas kortfattat tidigare satsningar på skydd av de elektroniska kommunikationerna. Dessa satsningar relateras sedan till dagens behov.

I **kapitel 4** redovisas ett till dagens förhållanden anpassat mål för skyddet av de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig. Det utgör en precisering som gjorts av PTS på grundval av de allmänna utgångspunkter för samhällets säkerhet och beredskap som redovisas i kapitel 2.

I kapitel 5, 6 och 7 redovisas på vilka sätt de elektroniska kommunikationerna bör skyddas. Vad som redovisas är en inriktning av kompletterande säkerhets-höjande åtgärder som bör genomföras eller upphandlas av staten med utgångspunkt i de elektroniska kommunikationer som skapas på marknadens villkor för normalt fredstida bruk.

I **kapitel 5** redovisas principer för samarbete om säkerhet mellan företrädare för allmänna intressen och enskilda aktörer inom elektronisk kommunikation.

I **kapitel 6** redovisas ett antal olika åtgärdsområden som PTS anser det angeläget att genomföra insatser inom. För varje sådant åtgärdsområde redovisas motiv för och syfte med åtgärderna, PTS inriktning av vad som bör göras samt exempel på insatser.

I **kapitel 7** redovisas allmänna grunder för prioritering av insatser.

Efter kapitel 7 följer en **litteraturförteckning**.

I **bilaga 1** återges en sammanfattning av den delrapport ”Telekommunikationernas sårbarhet och risker för samhället” som PTS insände till regeringen 2002-09-30 (diarienummer 02-12281). Huvudtexten i slutrapporten upprepar inte delrapportens resonemang men bygger med smärre modifieringar vidare på dess slutsatser.

I **bilaga 2** redovisas en komplettering till delrapporten som behandlar sårbarhet i distributionen av radio och TV och risker för samhället.

2 Politiska och organisatoriska utgångspunkter

Strategin grundar sig främst på statsmakternas beslut med anledning av propositionerna ”Fortsatt förnyelse av totalförsvaret” (prop. 2001/02:10) och ”Samhällets säkerhet och beredskap” (prop. 2001/02:158) samt på ”Förordning om åtgärder för fredstida krishantering och höjd beredskap” (SFS 2002:472) och ”Krisberedskapsmyndighetens planeringsinriktning för samhällets krisberedskap 2004”. Strategin har också så långt möjligt tagit hänsyn till det pågående arbetet med att utforma en ny lagstiftning för elektronisk kommunikation. PTS har också noterat de successiva förändringar i de säkerhetspolitiska utgångspunkterna som indikeras genom Försvarsberedningens rapport över den säkerhetspolitiska utvecklingen 2001 – 2003 ”Säkrare grannskap – osäker värld” (Ds 2003:8).

Dessa utgångspunkter innebär i sammandrag följande.

Enligt statsmakternas bedömning av det säkerhetspolitiska läget ter sig ett invasionshot mot landet inte möjligt inom minst en tioårsperiod förutsatt att vi har en grundläggande försvarsförmåga. Idag riskerar vi istället att hamna i en situation där händelser, som var för sig inte nödvändigtvis går att betrakta som krigshandlingar, utvecklas mot en krigsliknande situation. I ett sådant läge skapas en gråzon mellan krig och fred där osäkerheten kommer att vara stor. Utvecklingen av terrorism och militärteknik gör att insatser med stor förstörelsekraft och med utnyttjande av kvalificerad teknik kan tänkas förekomma från även andra än statliga aktörer.

Försvarsberedningen tonar i den nämnda rapporten ytterligare ned risken för väpnat angrepp och understryker betydelsen av Sveriges bidrag till fred och säkerhet i omvärlden samt behovet av att minska samhällets sårbarhet. Enligt Försvarsberedningen bedöms ett militärt väpnat angrepp i alla dess former från en annan stat direkt mot Sverige vara osannolikt under minst en tioårsperiod. Ett betydande antal konflikter med allvarliga följder i och utanför konfliktområdet bedöms dock komma att inträffa även i framtiden. De kan få konsekvenser för internationell fred och säkerhet och i förlängningen också för Sverige. Hot kan komma att riktas också mot det svenska samhället. Den tekniska infrastruktur som det moderna öppna samhället är beroende av blir i ökande grad transnationell och därmed en del av den gemensamma sårbarheten. Terroristgrupper kan via attacker mot IT-system, elförsörjning, telekommunikationer och ekonomiska system uppnå en del av de effekter på samhället och civilbefolkningen som det tidigare krävdes militära maktmedel för att uppnå.

Samhällets samlade behov av säkerhet och beredskap tillgodoses genom en helhetssyn på samhällets resurser och på att beredskapen skall byggas underifrån. Det innebär att utgångspunkten är den normala fredsverksamheten, vilken kompletteras med åtgärder inom ramen för säkerhets- och försvarspolitik.

Alla verksamhetsområden i samhället svarar i första hand själva för och finansierar själva sitt fredstida skydd och sin fredstida förmåga att hantera normalt förekommande störningar och påfrestningar. Därigenom skapas en basförmåga att tillgodose behovet av säkerhet och beredskap.

Staten svarar för att komplettera denna *basförmåga* med åtgärder för att hantera hela hotskalan från allvarliga fredstida kriser till höjd beredskap och krig. Därigenom skapas en *grundförmåga* att möta hot och påfrestningar omedelbart och på kort sikt samt en handlingsfrihet att kunna *anpassa* och om så krävs höja förmågan på medellång och lång sikt. Följande verksamheter kan därvid enligt gällande regler finansieras via statsbudgetens ”Utgiftsområde 6 Försvar samt beredskap mot sårbarhet”:

- investeringar avseende svåra påfrestningar på samhället i fred som samtidigt i hög grad stärker förmågan vid höjd beredskap,
- övnings- och utbildningsverksamhet som syftar till att ge samhället tillräcklig krishanteringsförmåga på lokal, regional och nationell nivå för såväl svåra påfrestningar på samhället i fred som höjd beredskap,
- investeringar för höjd beredskap samt
- viss internationell fredsfrämjande och humanitär verksamhet

Övrig statlig verksamhet för skydd och beredskap mot påfrestningar i fred skall i huvudsak finansieras via de ordinarie utgiftsområdena.

Strukturen för beredskapshänsyn och krishantering i samhället bygger på ett sektors- och ett områdesansvar. Sektorsansvaret utövas av särskilt förordnade centrala myndigheter. Områdesansvaret finns på tre nivåer i samhället – lokalt, regionalt och nationellt. På lokal nivå utövas områdesansvaret av kommunen, på regional nivå av länsstyrelsen och på nationell nivå av regeringen. En annan viktig aktör i sammanhanget är landstingen. Områdesansvaret har stor betydelse eftersom hantering av svåra påfrestningar i både fred och krig normalt kräver samverkan mellan flera sektorer.

I samhällets krishanteringssystem är tre principer centrala:

- ansvarsprincipen,
- likhetsprincipen och
- närhetsprincipen.

Ansvarsprincipen innebär att den som har ansvar för en verksamhet under normala förhållanden skall ha motsvarande ansvar under kris- och krigssituationer. Likhetsprincipen innebär att en verksamhets organisation och lokalisering så långt som möjligt skall överensstämja i fred, kris och krig. Närhetsprincipen innebär i sin tur att kriser skall hanteras på lägsta möjliga nivå i samhället.

Krisberedskapsmyndigheten har under regeringen ansvar för att samordna arbetet med samhällets beredskap inför allvarliga kriser.

Ett antal samverkansområden har inrättats för att förbättra och utveckla förmågan att hantera kriser som berör flera sektorer. Inom Samverkansområdet teknisk infrastruktur (SOTI) samverkar Affärsverket svenska kraftnät, Elsäkerhetsverket, Krisberedskapsmyndigheten, Livsmedelsverket, Post- och telestyrelsen, Statens energimyndighet och Statens kärnkraftinspektion för att samhällsviktiga behov av den tekniska infrastrukturen skall kunna tillgodoses vid allvarliga fredstida störningar och i krig. Även Styrelsen för psykologiskt försvar har adjungerats till samverkansområdet.

Post- och telestyrelsen har inom samverkansområdet Teknisk infrastruktur tillsammans med andra ingående myndigheter ett särskilt ansvar såväl för att planera och vidta förberedelser för fredstida krishantering som för att vidta de förberedelser som behövs inför och vid höjd beredskap. Myndigheten skall samverka med andra berörda myndigheter, landsting, kommuner, näringsliv och organisationer.

De elektroniska kommunikationerna har tillsammans med elförsörjningen central betydelse för att samhällsviktig verksamhet skall fungera vid svåra påfrestningar i fred, höjd beredskap och krig. Det är viktigt att inom dessa områden planera för att minska sårbarheten och öka robustheten i de extraordinära situationerna.

Svenska samhällets reglering vad gäller de elektroniska kommunikationerna håller för närvarande på att förändras. Enligt regeringens förslag i prop 2002/03:110 Lag om elektronisk kommunikation 2003 föreslås följande mål för sektorn elektronisk kommunikation.

”Enskilda och myndigheter skall få tillgång till effektiva och säkra elektroniska kommunikationer. De elektroniska kommunikationerna skall ge största möjliga utbyte när det gäller urvalet av överföringstjänster samt deras pris och kvalitet. Sverige skall i ett internationellt perspektiv ligga i framkant i dessa avseenden. De elektroniska kommunikationerna skall vara hållbara, användbara och tillgodose framtidens behov. De främsta medlen för att uppnå detta är att skapa förutsättningar för en effektiv konkurrens utan snedvridningar och begränsningar samt att främja internationell harmonisering. Staten skall ha ett ansvar på områden där allmänna intressen inte enbart kan tillgodoses av marknaden.”

Bland områden där staten skall ha ett ansvar anges i prop. 2002/03:110 uthållighet och tillgänglighet vid extraordinära händelser i fredstid, höjd beredskap och krig.

3 Skydd av de elektroniska kommunikationerna förr och nu

3.1 Tidigare satsningar

Sedan länge har det varit av stor betydelse att inom det svenska totalförsvaret ha tillgång till fungerande telekommunikationer vid höjd beredskap och krig. Omfattande insatser har därför successivt genomförts för att minska systemens sårbarhet och skapa förutsättningar för fungerande kommunikationer också i krig.

Den bedömda hotbild som låg till grund för satsningarna under 1990-talet var främst flygbekämpning med precisionstyrda vapen. Möjligheterna att nå verkan med sådana vapen hade tydligt illustrerats under Gulfkriget och bedömningen gjordes att de ganska stora mål som tidigare telefonväxlar i byggnader utgjorde skulle vara troliga mål för bekämpning vid ett angrepp mot Sverige.

Under de senaste tio åren har stora investeringar genomförts för att förlägga viktiga växlar och centrala delar av transmissionsnät och styrsystem i fullträffsskyddade utrymmen i form av berggrum. Detta gällde inledningsvis främst Telias nät för fast telefoni men har efterhand utvidgats till att omfatta även system för mobiltelefoni och andra operatörer. I dag finns ett tjugotal operatörer i de berggrum PTS investerat i.

Även andra åtgärder har vidtagits för att minska sårbarheten och öka robustheten bl.a. förstärkning av reservkraften. Redundansen i det samlade kommunikationsnätet har också blivit större genom beslut på företagsnivå vilket resulterat i maskformighet i näten, tillväxt av mobiltelefoni och datanät samt tillkomst av fler operatörer.

Det finns således en värdefull grund att bygga vidare på för att fortsatt säkerställa skyddet av de elektroniska kommunikationerna. Samtidigt är förutsättningarna i många avseenden nya. Den säkerhetspolitiska situationen är starkt förändrad samtidigt som teknik och marknad utvecklas snabbt.

3.2 Dagens behov

Ett invasionshot mot Sverige ter sig inte möjligt under minst en tioårsperiod förutsatt att Sverige har en grundläggande försvarsförmåga. Begränsade angrepp med militära medel mot mål i Sverige kan dock fortfarande inte helt uteslutas. Samtidigt har andra typer av hot från kriminella grupper, terrorister och icke-demokratiska stater även långt från Sverige blivit mer påtagliga. Samhället kan också utsättas för svåra påfrestningar genom andra extraordinära omständigheter.

Den tekniska utvecklingen inom informationsteknologi och telekommunikationer har gått mycket snabbt vilket bl.a. medfört en kraftig tillväxt av de elektroniska kommunikationerna och samhällets beroende av dem. Centralisering och fjärrstyrning av trafiken gör all elektronisk kommunikation, även den lokala, alltmer beroende av fungerande förbindelser till några få ofta avlägsna styrnoder och växlar, vad gäller Internet i många fall även utanför landet.

De många förändringarna gör sammantaget att det behövs en ny strategi för hur skyddet för de elektroniska kommunikationerna i fortsättningen skall tillgodoses.

4 Mål för skyddet av de elektroniska kommunikationerna

Målet är att de elektroniska kommunikationerna skall vara uppbyggda på ett sådant sätt

- att kriser i fred inte leder till oacceptabla avbrott eller störningar
- att konsekvenser av svåra påfrestningar minimeras och
- att förmågan på fem till tio års sikt kan anpassas till de krav som ställs i ett förändrat säkerhetspolitiskt läge

Inriktningen (av PTS åtgärder) att nå målet/målen är att säkerställa tillförlitligheten, uthålligheten och tillgängligheten samt öka robustheten i de elektroniska kommunikationssystemen. På så sätt minskas sårbarheten.

Målformuleringen utgår från principen att uthållighet, ökad motståndskraft och ett robust system för elektronisk kommunikation byggs underifrån. I såväl privata som statliga aktörers nät finns inbyggt en basnivå vad gäller säkerhet och uthållighet. Denna basförmåga bestäms huvudsakligen utifrån kommersiella överväganden på en marknad. Därutöver kompletteras denna förmåga med statligt beslutade och finansierade åtgärder. Strävan skall vara att de åtgärder som vidtas är till nytta för såväl fredstida kriser som krig.

Tänkbara hot i fredstid som skyddet för de elektroniska kommunikationerna skall utformas mot är främst mycket extrema vädersituationer, svåra olyckor, terroristangrepp med fysiska eller elektroniska medel eller genom biologisk eller kemisk kontaminering samt informationsoperationer.

Vid svåra påfrestningar på samhället i fred skall de elektroniska kommunikationerna ha sådant skydd att de uthålligt kan medverka till att viktiga samhällsfunktioner kan upprätthållas. Sådana funktioner är bl.a. ledning, polis, räddningstjänst, vård och omsorg, försörjning med livsmedel, vatten och värme, elförsörjning, viktiga transporter av personer och varor, betalningsväsende och massmedial information. Däremot är det rimligt att vid en svår påfrestning acceptera t.ex. vissa avbrott i produktionen. Allmänhetens behov av information och möjligheter till kommunikation för att kunna hantera den uppkomna krissituationen måste dock tillmätas stor vikt.

Tänkbara hot vid höjd beredskap och krig som skyddet skall utformas mot är omedelbart eller i närtid främst insatser från sabotörer eller begränsade angrepp med militära medel mot de elektroniska kommunikationerna. En möjlighet skall finnas att på fem till tio års sikt anpassa skyddet så att det svarar mot även mer omfattande och andra typer av angrepp.

Vid hotande väpnat angrepp eller i krig skall de elektroniska kommunikationerna i första hand kunna medverka till att säkerställa livsnödvändiga funktioner och till att möjliggöra ett effektivt försvar.

Sverige skall också kunna ställa civil kompetens och civila resurser inom elektronisk kommunikation till förfogande för internationell krishantering.

Det här redovisade målet för skyddet av de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig utgör en precisering som PTS gjort på grundval av de allmänna utgångspunkter för samhällets säkerhet och beredskap som redovisats i kapitel 2.

I följande tre kapitel redovisas sätt att nå dessa mål.

5 Principer för samarbete

Det primära sättet att tillgodose skyddet av de elektroniska kommunikationerna skall vara att inom ramen för landets samlade satsning på krisberedskap utveckla ett samarbete om säkra elektroniska kommunikationer mellan företrädare för stat och kommun och enskilda aktörer inom elektronisk kommunikation. PTS, andra myndigheter inom Samverkansområdet teknisk infrastruktur, Försvarmakten samt länsstyrelser och kommuner utgör de viktigaste företrädarna för stat och kommun.

Samarbetet ska utgå från de former för elektronisk kommunikation som under normala förhållanden och fri konkurrens växer fram i samhället. PTS syfte med samarbetet med enskilda aktörer är att öka medvetenheten om de svåra situationernas krav och att finna lämpliga kompletterande åtgärder för att tillgodose skyddet för de elektroniska kommunikationerna i fred och vid höjd beredskap och krig. Genom kompletterande åtgärderna skall riskerna minskas för att störningar skall leda till sämre tillförlitlighet, uthållighet och tillgänglighet samt att förutsättningar skapas för att samhället skall kunna hantera situationer när sådana brister trots allt uppstår.

Staten skall genom PTS i partnerskap samverka med de enskilda aktörerna inom elektronisk kommunikation med utnyttjande av ekonomiska incitament och överenskommelser till gemensam nytta. Information, granskningsinsatser, branschstandarder, gemensamma krisövningar och praktiska försök utgör viktiga medel för koordinering och samverkan.

Samarbete skall sökas med myndigheter representerade inom Samverkansområdet teknisk infrastruktur, Försvarmakten, länsstyrelser och kommuner samt andra myndigheter med stor betydelse för eller beroende av de elektroniska kommunikationerna. Samverkan skall även omfatta operatörer inom elektronisk kommunikation men också aktörer inom elförsörjning och elektronisk mediedistribution. PTS avser att verka för att olika myndigheters och andra organs roller inom sektorn i extraordinära situationer förtydligas.

Strävan skall vara att söka upphandla de kompletterande säkerhetshöjande insatser som behövs i samband med utbyggnad, nybyggnation och reinvestering inom systemen för elektronisk kommunikation.

Åtgärder för att öka säkerheten i de svåra situationerna 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 skall vara att genom partnerskap nå uppgörelser om samfinansiering mellan staten och enskilda aktörer om åtgärder av värde för säkerheten såväl i fred, som höjd beredskap och krig.

Som komplettering till överenskommelser med marknadens aktörer om ökad säkerhet kan PTS vid behov utnyttja de möjligheter som lagen ger att

förpliktiga operatörer av särskild betydelse från allmän synpunkt att på visst sätt beakta totalförsvarets behov av elektronisk kommunikation under höjd beredskap.

PTS skall till regeringen lämna förslag till åtgärder av författningsmässig eller annan natur, som myndigheten inte själv kan besluta om och som behövs för att tillgodose tillförlitlighet, uthållighet och tillgänglighet hos de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig.

6 Åtgärdsområden

Nedan presenteras ett antal områden som PTS anser det angeläget att genomföra insatser inom för att stärka skyddet för de elektroniska kommunikationerna.

Valet av områden grundar sig på en bedömning av en mängd faktorer bl.a. de påtagliga hot mot de elektroniska kommunikationerna som finns också i dagens säkerhetspolitiska läge, svaga punkter i dagens system, behovet av att ansluta till pågående utbyggnad av nät med hög överföringskapacitet, samhällets alltmer utbredda beroende av elektroniska kommunikationer, behovet av också mjuka kunskapsorienterade insatser och att utöver förebyggande insatser också satsa på förmåga att hantera störningar om de trots allt uppkommer.

Åtgärder inom ett antal av dessa områden (stimulans och information till aktörer, stöd med vissa tjänster, internationellt samarbete, övningar och uppföljning) är relativt billiga. De bedöms ge hög effekt om än med begränsad varaktighet. Upprepade insatser är därför nödvändiga.

Andra områden (utbyggd redundans och flexibilitet, elförsörjningen och skydd mot informationsintrång) förutses kräva mer omfattande resurser och investeringar.

6.1 Stimulans till ett ökat användaransvar inom elektroniska kommunikationer

Samhällsviktiga funktioner skall stimuleras att vidta åtgärder för att skapa god säkerhet i sina egna telekommunikationer redan vid normalt förekommande störningar. Därigenom skapas den basförmåga som skyddet även i svåra situationer måste bygga på.

6.1.1 Syfte

Olika användarkategoriernas krav på funktionssäkerhet hos de elektroniska kommunikationerna varierar. Vissa användare klarar utan större olägenheter relativt långa avbrott och betydande kvalitetssänkningar i de tjänster som erbjuds. Andra användare har små eller inga toleranser.

Eftersom full säkerhet mot alla tänkbara hot aldrig kan uppnås kommer det att finnas en risk att de gemensamma satsningar som görs på funktionssäkerhet i de elektroniska kommunikationerna inte är tillräckliga i förhållande till de krav som enskilda användare har. Dessutom är det inte en realistisk ambition att anpassa den generella säkerhetsnivån i elektroniska kommunikationer efter användare med de högsta kraven på funktionssäkerhet.

Det är i första hand den enskilda användarens 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. Genom att alla verksamheter som är beroende av elektronisk kommunikation tar ansvar för sin egen vardagssäkerhet skapas över landet en basförmåga och en grundläggande robusthet samt beredskap att motstå hot och hantera störningar.

Detta åtgärdsområde syftar till att stimulera samhällsviktiga verksamheter att skapa en god basförmåga och robusthet i sina elektroniska kommunikationer. Därmed förbättras de grundläggande förutsättningarna för att samhällsviktiga verksamheter skall kunna ha tillgång till uthålliga och tillförlitliga elektroniska kommunikationer också i samband med svåra påfrestningar på samhället i fred, höjd beredskap och krig.

6.1.2 Inriktning

I första hand skall åtgärderna inriktas på att samhällsviktiga verksamheter själva skall vidta åtgärder för att tillgodose den egna tillgången till lämpliga

elektroniska kommunikationer. En viktig möjlighet som PTS avser att utnyttja i detta sammanhang är att informera om hur man drar fördel av den redundans som kan skapas genom att utnyttja flera av de olika typer kommunikation och operatörer som marknaden erbjuder.

Åtgärderna inom detta område skall främst omfatta analyser, information och rådgivning. Detta ställer krav på tillgång till personella resurser, något som PTS kan tillgodose genom att anställa personal alternativt genom upphandling av tjänster.

PTS avser att genomföra åtgärder inom detta område tillsammans med marknaden och andra aktörer inom Samverkansområdet för teknisk infrastruktur.

6.1.3 Lämpliga åtgärder

6.1.3.1 Information och rådgivning

För vissa användare kan det vara alltför kostsamt att hålla med egen kunskap hur man skall säkerställa sina elektroniska kommunikationssystem. PTS kan tillhandahålla information och rådgivning i frågor som rör elektroniska kommunikationer med avseende på säkerhet och beredskap.

Detta kan ske genom allmän information i syfte att öka medvetenheten och driva på utvecklingen inom området. I första hand bör PTS inrikta sig på att sprida kunskap bland dem som arbetar med säkerhet och genomför säkerhetsanalyser.

Det kan även ske behovsstyrt då användare vänder sig till PTS. En del i arbetet innebär att PTS profilerar sig som en kontaktpunkt för all samhällsviktig verksamhet i frågor som rör elektronisk kommunikation.

6.1.3.2 Säkerhetsanalyser

Ett sätt att aktivt medvetandegöra brister i elektroniska kommunikationssystem är att genomföra säkerhetsanalyser hos samhällsviktiga verksamheter. Till skillnad från Krisberedskapsmyndigheten och kommunerna så har PTS inget övergripande ansvar för att granska samhällsviktig verksamhets säkerhet. Det är ändå viktigt att PTS tar initiativ till samverkan i samband med att granskningar genomförs och då speciellt beaktar de elektroniska kommunikationerna. (Jämför även med liknande åtgärd för operatörer under åtgärdsområdet Stöd till satsningar på inre säkerhet.)

6.1.3.3 Medverkan i uppföljningsstudier

Erfarenheter som visar hur större störningar drabbar användare bör spridas till andra användare. Detta underlag är även användbart för PTS som underlag för prioritering av åtgärder. Det är därför viktigt att ta initiativ till och medverka i uppföljningsstudier som genomförs och då utreda vilka konsekvenser större

störningar har för de användare som drabbades. (Jämför med motsvarande åtgärd under åtgärdsområdet 6.9 Granskning av vilken funktionssäkerhet som uppnås i näten.)

6.2 Ökad redundans och flexibilitet i nätverk

De elektroniska kommunikationernas känslighet för samtidigt förekommande störningar skall minskas.

Kompletterande insatser skall göras för att öka redundansen i näten utöver vad som är kommersiellt motiverat så att samhällsviktiga behov av elektronisk kommunikation säkrare kan tillgodoses i de extraordinära situationerna. Möjligheterna skall tas tillvara att ansluta till den pågående utbyggnaden av IT-infrastruktur med hög överföringskapacitet.

Det är angeläget att finna tekniskt och ekonomiskt rimliga former för att under extraordinära förhållanden kunna utnyttja den redundans som överkoppling mellan olika operatörers nät skulle skapa.

Fortsatta studier avseende möjligheter att prioritera trafik i telenätet ska genomföras.

Försvarsmaktens behov av tillgång till de civila näten skall uppmärksammas.

6.2.1 Syfte

En konsekvens av att nätfunktioner och tjänster fortlöpande centraliseras och att näten i allt större utsträckning fjärrövervakas och fjärrstyrs är en ökad risk för att delar av landet kan bli telemässigt avskurna vid stora skador i transmissionsnäten. Brutna förbindelser med centrala delar av nätet kan innebära att inte ens lokala kommunikationer kan upprätthållas. Risken är särskilt stor för Norrland och Gotland, liksom i andra geografiskt svårtillgängliga delar av landet med begränsat befolkningsunderlag. Den kommersiella utvecklingen för dessa områden har inte inneburit utbyggd redundans i samma utsträckning som i övriga delar av landet.

Detta åtgärdsområde syftar i huvudsak till att göra nätverken för elektroniska kommunikationer mer robusta vid extraordinära situationer. Risken för samtidigt förekommande störningar på flera ställen är då särskilt stor.

6.2.2 Inriktning

Åtgärderna inom detta område skall inriktas mot att dels öka redundansen i näten och dels skapa förutsättningar för att kunna utnyttja de omkopplingsmöjligheter som de tekniska systemen medger. Det handlar då inte i första hand om en redundans för enstaka störningar utan om en beredskap för mer omfattande händelser. Samtidiga och mer omfattande störningar är mycket

sällsynta under normala förhållanden men är typiska för svåra påfrestningar i fred, höjd beredskap och krig.

I en krissituation, som inte nödvändigtvis primärt behöver drabba de elektroniska kommunikationerna, är man beroende av fungerande kommunikationer för att kunna hantera krisen. Detta ställer krav på förberedelser för att funktionen skall kunna upprätthållas trots störningar i samhället.

Omfattande investeringar kommer att erfordras framför allt för att öka redundansen och flexibiliteten i nätverken så att även mer omfattande och avsiktliga störningar kan hanteras. Insatser skall särskilt inriktas mot den pågående utbyggnaden av IT-infrastruktur med hög överföringskapacitet. Genom att i samband med utbyggnad påverka nätens uppbyggnad och göra kompletterande investeringar kan minskad sårbarhet och ökad robusthet uppnås på ett kostnadseffektivt sätt. Lokala åtgärder bör samordnas på regional nivå och ingå i en större plan för att PTS skall kunna ta ställning till dem.

Av stort intresse för att kunna hantera svåra störningar är att söka utveckla möjligheter till prioritering och finna tekniskt och ekonomiskt rimliga möjligheter till hopkoppling i krissituationer mellan olika operatörens nät.

PTS skall samverka med Försvarsmakten för att klarlägga Försvarsmaktens och det nätverksbaserade försvarets behov av tillgång till redundanta förbindelser i de civila näten.

Vid satsningar på åtgärder för att förbättra redundans och flexibilitet i nätverk för elektronisk kommunikation skall följande fyra förhållanden särskilt beaktas:

- **Platser med stor sannolikhet att drabbas av störningar.** Det är rimligt att satsningar görs där störningar i extraordinära situationer har större sannolikhet att inträffa. Vilka störningar som kan inträffa beror på hotbilden. Vissa delar av landet är exempelvis mer utsatta för extremt väder, vissa platser kan vara mer intressanta som mål för sabotage och terrorism. Militära hot behöver PTS närmare utvärdera i samarbete med Försvarsmakten.
- **Sårbara komponenter.** Vissa komponenter i de elektroniska kommunikationssystemen är mer centrala för systemens funktion.
- **Samhällsviktiga funktioners behov.** Närvaro av samhällsviktiga funktioner kan motivera speciella satsningar på redundans. Det kan vara verksamhet som är viktig på lokal, regional eller nationell nivå.
- **Antal drabbade abonnenter.** För att begränsa påfrestningarna på samhället är det viktigt att så få människor som möjligt drabbas vid extraordinära störningar.

6.2.3 Lämpliga åtgärder

En del av åtgärderna inom detta område kan innebära att PTS upphandlar utrustning och tjänster som leder till en minskad sårbarhet och ökad robusthet. Andra åtgärder innebär att PTS driver arbetet i nära samarbete med operatörer och nätägare.

6.2.3.1 Utveckling av möjligheter till prioritering

I en kris kan det vara många användare som samtidigt vill utnyttja de elektroniska kommunikationerna, samtidigt som skador på nät kan ge en begränsad kapacitet. Det kan då vara viktigt att samhällsviktiga användare ges en högre prioritet och således ökad möjlighet att kommunicera för att hantera krissituationen. PTS kommer att fortsätta arbetet med att studera möjligheterna till införande och utveckling av tjänster för prioritering samt möjligheterna till implementering..

6.2.3.2 Extra noder

Genom att tillföra extra noder som avlastar eller speglar andra noder kan man reducera eller eliminera effekten av att noder faller bort. Detta kan ske genom att man tillför permanenta noder, exempelvis upphandling av alternativa styr- och övervakningsplatser. Man kan även tänka sig att tillhandahålla flyttbara noder som kan flyttas till en plats där man anser att de behövs. Exempel på detta är upphandling av mobila radiobasstationer.

Idag finns ett flertal nätägare med egna nät. Genom att tillföra hopkopplingspunkter och länkar mellan dessa nät skulle man kunna få en ökad redundans.

6.2.3.3 Extra länkar

Nya länkar ger nya maskor i näten och ger möjlighet att koppla runt skadade delar av näten. Man kan här tänka sig länkar av permanent och mobil/tillfällig karaktär. Med radiolänkutrustning kan man relativt snabbt upprätta en tillfällig länk där så behövs.

Det är viktigt att följa upp så att ny fiber inte läggs längs redan existerande sträckningar, utan att man väljer nya vägar för att få fler fysiskt åtskilda maskor i näten.

Investeringar i extra noder eller länkar kan genomföras dels grundat på PTS egen analys, men det är även önskvärt att operatörer och nätägare bidrar med sin kunskap och erfarenhet. Operatörerna måste därför informera PTS när de arbetar med denna typ av åtgärder.

6.2.3.4 Samutnyttjande av nät vid extraordinära situationer

Det finns idag ett flertal nät för elektroniska kommunikationer vilka ägs av olika aktörer. Hopkoppling av dessa nät ger potentiellt goda möjligheter till ökad redundans. Det är därför angeläget att närmare utreda vilka teknisk och ekonomiskt rimliga möjligheter som står till buds och vilka överenskommelser

mellan operatörerna som krävs för att man snabbt skall kunna samutnyttja nät om skador i näten uppstår.

6.2.3.5 Tester och övningar

För att säkerställa tillräcklig redundans måste det initieras tekniska tester där möjligheter till omkoppling utvärderas. Likaså måste samövningar mellan operatörer genomföras som säkerställer att även samarbete mellan operatörer i kritiska situationer fungerar.

6.2.3.6 Anpassningsåtgärder

PTS kommer att verka för att anpassningsplaner med avseende på ökad redundans för att uppnå önskvärd förmåga på medellång sikt (inom fem år) utarbetas. För en angiven åtgärd skall det specificeras varför och när en sådan åtgärd behöver genomföras. Planerna kommer efter hand att rapporteras till Krisberedskapsmyndigheten som har ett samordnande ansvar för anpassningsåtgärder.

6.3 Förbättrat skydd mot både fysiska och elektromagnetiska hot

De viktigaste delarna som för närvarande existerar av nätverken har placerats i anläggningar som skyddar mot fysisk och elektromagnetisk åverkan. Fortsatta investeringar i dessa anläggningar handlar mer om att utveckla dem mot nya krav än om regelrätta omfattande utbyggnader. Övriga viktiga noder i nät med hög överföringskapacitet som inte är förlagda i berggrum behöver också skyddas mot skador på grund av svåra olyckor och avsiktlig skadegörelse. PTS skall vid behov upphandla förstärkning av skyddet utöver vad som är kommersiellt motiverat.

6.3.1 Syfte

De elektroniska kommunikationerna utgörs av tekniska system, placerade på platser som ofta är lätt fysiskt åtkomliga, de har dessutom en stor geografisk utbredning. Detta gör dem utsatta för slumpmässiga hot och åtkomliga för avsiktliga angrepp.

Förbättrat skydd skall hindra eller begränsa effekten av direkta fysiska hot. Det skall även för de mest väsentliga noderna ges skydd mot elektromagnetisk puls. Syftet är att minska risken att kritiska delar av de elektroniska kommunikationssystemens infrastruktur slås ut under en längre tid. Målet är att försvåra terroristinsatser, sabotage och angrepp mot vitala delar av systemen för elektronisk kommunikation så att sådana angrepp ter sig riskfyllda eller kostnadskrävande i förhållande till det resultat som kan uppnås.

6.3.2 Inriktning

Det fysiska skyddet för centrala delar av systemen för elektronisk kommunikation har under senare år givits ett mycket gott skydd genom förläggning i berggrum. Fortsatta åtgärder skall ta hänsyn till detta och i första hand dra nytta av de resurser som redan har byggts ut. Tillkommande centrala ledningsorgan och viktiga noder i nät med hög överföringskapacitet skall uppmärksammas. Övriga viktiga noder som idag inte finns i berggrum bör skyddas från skador som kan uppkomma på grund av svåra olyckor eller skadegörelse.

Liksom för åtgärdsområdet 6.2 Ökad redundans och flexibilitet i nätverk avser PTS att prioritera satsningar på åtgärder för förbättrat skydd i extraordinära situationer efter beaktande av följande fyra förhållanden:

- Platser med stor sannolikhet att drabbas av störningar
- Sårbara komponenter
- Samhällsviktiga funktioners behov

- Antal drabbade abonnenter.

Det är viktigt att notera att ökad redundans kan vara ett alternativ till ett förbättrat skydd. En kritisk systemkomponent blir mindre sårbar om den skyddas och mindre kritisk om den dubblas. Utspridning och många möjligheter till vägval i maskformiga nät kan ge säkrare elektroniska kommunikationer än bra skydd för centrala noder i hierarkiska nät. PTS kommer att beakta detta, liksom kostnaderna för olika alternativ.

6.3.3 Lämpliga åtgärder

6.3.3.1 Förstärkt tekniskt skalskydd

Utrustning av stor betydelse kan vid behov ges ett förstärkt tekniskt skalskydd. Detta skydd bör vara hotbildsanpassat. Investeringar i förbättrat skydd bör endast avse extraordinära händelser som kan ge stora konsekvenser för samhället. Exempel på åtgärder kan vara kompletterande insatser för att ge viktiga noder skydd i bergrum samt upphandling av skydd mot elektriska och elektromagnetiska hot.

6.3.3.2 Anpassningsåtgärder

PTS kommer att verka för att anpassningsplaner med avseende på förbättrat skydd för att uppnå önskvärd förmåga på medellång sikt (inom fem år) utarbetas. För en angiven åtgärd skall det specificeras varför och när en sådan åtgärd behöver genomföras. I detta arbete kan ingå att kartlägga viktiga noder. Planering för situationsanpassade bevakningsåtgärder kan även ingå i denna planering.

6.4 Minskad känslighet för informationsoperationer samt åtgärder för att motverka sådana

De informationsteknologiska hoten mot elektroniska kommunikationer skall ägnas särskild uppmärksamhet. PTS skall i sitt arbete med IT-säkerhet och i samverkan med andra berörda aktörer i samhället beakta de svåra angrepp mot elektroniska kommunikationer och andra allvarliga störningar som kan förekomma i fred, höjd beredskap och krig. Insatserna bör omfatta analyser, tekniska tester och information och investeringar för att försvåra kvalificerade informationsteknologiska angrepp.

6.4.1 Syfte

Informationsoperationer, som intrång i och manipulation av informationssystem, är ett hot som växer i takt med att det svenska samhällets beroende av informationssystem ökar. Denna typ av angrepp kan rikta sig direkt mot de elektroniska kommunikationssystemen, men även utnyttja dessa system för att angripa andra samhällsviktiga funktioner. Det är därför viktigt att det vidtas åtgärder inom detta område så att de elektroniska kommunikationssystemen har en hög tillförlitlighet, uthållighet och tillgänglighet i fredstida kriser, höjd beredskap och krig.

6.4.2 Inriktning

PTS har ansvaret för Sveriges IT-incidentcentrum (SITIC). Denna har en viktig roll såväl i det fredstida IT-säkerhetsarbetet som i skyddet mot informationsoperationer. Funktionen kan motverka angrepp genom att varna och informera myndigheter och företag om sårbarheter och skyddsåtgärder och genom att ge dem stöd i att införa skydd mot IT-incidenter. Funktionen kan också analysera rapporter om inträffade incidenter för att bland annat kunna skilja systematiska angrepp från den stora mängden okvalificerade angrepp.

Utöver detta allmänna uppdrag för IT-incidentfunktionen kommer PTS verka för att minska de elektroniska kommunikationernas känslighet för informationsoperationer.

PTS ser ett behov av att det utarbetas en samordnad svensk strategi för att bemöta en situation då domännamnsystemet utsätts för påfrestningar. Denna strategi bör utarbetas i samverkan mellan berörda myndigheter och organisationer. PTS är berett att initiera och leda ett sådant samarbete. Se vidare beträffande Internet PTS rapport ”Är Internet i Sverige robust?” (PTS-ER-2003:1).

Inom detta åtgärdsområde förutser PTS ett behov av ökade insatser för att förbättra skyddet mot kvalificerade angrepp.

6.4.3 Lämpliga åtgärder

6.4.3.1 Bidra till höjd säkerhetsnivå

Genom IT-incidentfunktionens verksamhet kommer PTS att bidra till ett ökat skydd mot informationsoperationer och informationskrigföring. Genom information till operatörer och nätägare avser PTS att sprida kunskap och uppmuntra till samarbete.

6.4.3.2 Tekniska tester

Tekniska tester är en metod för att utvärdera de elektroniska kommunikationernas skydd mot IT-relaterade hot.

6.4.3.3 Tekniska åtgärder

För att minska känsligheten för informationsoperationer bör man utvärdera och bidra till tekniska åtgärder för att minska de elektroniska kommunikationernas känslighet för informationsoperationer. Ett intressant område kan vara att studera möjligheten att införa filter på nationell nivå. Sådana filter skulle möjligen kunna begränsa omfattningen av exempelvis överbelastningsattacker mot DNS-systemet.

6.4.3.4 Standarder

Det är viktigt att bidra till utveckling av standarder gällande exempelvis teknisk utrustning, riktlinjer för incidentrapportering, kryptering, certifiering och säkerhetsnivåer gällande skydd mot IT-relaterade hot.

6.5 Säkrare elförsörjning och fördjupat samarbete mellan el- och teleområdena

De elektroniska kommunikationerna är beroende av en fungerande elförsörjning. Samhället kräver i sin tur fungerande elektroniska kommunikationer vid störningar i elförsörjningen. Det ömsesidiga beroendet kräver att samarbetet fördjupas och utvecklas mellan ansvariga myndigheter och operatörer inom el- och teleområdena. Ytterligare satsningar skall göras att minska konsekvenserna av det ömsesidiga beroendet vid avsiktliga angrepp och omfattande störningar i systemen.

Det kommer att behövas avsevärda investeringar för att minska riskerna för att störningar i elförsörjningen skall störa de elektroniska kommunikationerna.

Det är inte möjligt att säkerställa en helt störningsfri elförsörjning. Samtidigt ökar elberoendet i samhället, bland annat till följd av ett ökat krav på fungerande elektroniska kommunikationer och IT-system. Ett allvarligt hot mot de elektroniska kommunikationerna i fred är långvariga avbrott i elförsörjningen. Sådana avbrott drabbar normalt många funktioner i samhället. Avbrott kan exempelvis orsakas av extremt väder, tekniska fel eller omfattande sabotage eller terroristangrepp.

Det finns ett ömsesidigt beroende mellan de elektroniska kommunikationerna och elförsörjningen. Vid störningar i elförsörjningen är fungerande elektroniska kommunikationer väsentliga för att kunna hantera problemen, såväl inom elförsörjningen i sig som inom verksamheter som drabbas av brister i elförsörjningen. Regeringen har uppdragit åt Statens energimyndighet att se till att en helhetssyn utvecklas som omfattar beredskapsåtgärder såväl på den el-operativa sidan som på användarsidan och att åtgärder skall vägas emot varandra gällande kostnader och effekt. PTS deltar i detta arbete.

Åtgärder inom detta område syftar till att skapa en säkrare elförsörjning för de elektroniska kommunikationerna vid svåra påfrestningar på samhället i fred, höjd beredskap och krig. Säkrare elförsörjning till elektroniska kommunikationer ingår som en integrerad del i en förbättrad elförsörjning för samhället i stort. Den är väsentlig för att minska konsekvenserna för samhället av störningar i elförsörjningen. Ett fördjupat samarbete mellan el- och teleområdena är ett viktigt medel för att minska sårbarheten mot störningar inom båda områdena.

6.5.1 Inriktning

PTS samarbetar med Svenska Kraftnät, Statens Energimyndighet och andra aktörer på el- och telemarknaden för att minska risken för störningar och att i

en extraordinär situation så långt som möjligt kunna vidmakthålla nödvändig kommunikation och elförsörjning. PTS medverkar också i HEL-projektet.

En struktur för ömsesidigt informations- och erfarenhetsutbyte om bland annat beredskapsåtgärder och förändringar bör utvecklas för att förbättra och snabba upp kontakten mellan representanter för el- och teleområdena. Samverkansområdet för teknisk infrastruktur är ett lämpligt forum för att initiera denna typ av arbete.

Samarbetet mellan el- och teleområdena bör leda till ett gemensamt planerings- och analysarbete. Genom att samordna åtgärder för att höja beredskapen inom såväl el som elektroniska kommunikationer är förhoppningen att man kan utnyttja respektive systems styrka och minimera dess svaghet på ett mer effektivt sätt. Denna samverkan bör även innefatta planering för krishantering. Viktigt är också att uppmärksamma de behov av elektroniska kommunikationer som finns inom elförsörjningen i samband med kraftiga störningar i elproduktionen.

PTS bedömer att behovet av investeringar kommer att öka för att uppnå en säkrare elförsörjning för de elektroniska kommunikationerna i extraordinära situationer.

6.5.2 Lämpliga åtgärder

6.5.2.1 Investeringar i säkrare elförsörjning

Satsningar på lösningar för reservkraft och alternativa matningsvägar bör ske i nära samarbete med representanter för elområdet och teleoperatörerna. Bland annat går det att överväga lokala lösningar där geografiskt närliggande intressenter i en säker elförsörjning arbetar tillsammans.

Om gemensamma intressen finns från såväl el- som teleområdet anser PTS att det borde vara möjligt att samfinansiera åtgärder.

6.5.2.2 Gemensamma tester och övningar

Övningar och tester där representanter från både el- och teleoperatörer deltar främjar förståelse och samarbete, samt höjer medvetenheten om det ömsesidiga beroendet mellan dessa båda infrastruktursystem.

6.6 Stöd till satsningar på inre säkerhet

Den inre säkerheten har stor betydelse redan under normala förhållanden och måste i första hand vara operatörers och nätägares ansvar. PTS ska verka för att med information, råd och stöd.

Olika nätägare och operatörer men också användarna av elektronisk kommunikation skall uppmärksammas på betydelsen av inre säkerhet. Operatörer och nätägare med säkerhetskänslig verksamhet bör kontrollera möjligheter 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.

6.6.1 Syfte

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 angripa de elektroniska kommunikationernas funktion måste ha en mycket ingående kännedom om systemens uppbyggnad. Detta gör att den inre säkerheten hos olika operatörer men också hos användarna av elektronisk kommunikation får allt större betydelse. Personer med tillträde, så kallade insiders, skulle kunna orsaka stora störningar genom att utnyttja sin kunskap och sina möjligheter att påverka för att skada de elektroniska kommunikationerna.

Detta åtgärdsområde syftar till att stärka den inre säkerheten inom alla verksamheter som utnyttjar eller tillhandahåller elektronisk kommunikation för att begränsa möjligheterna till insyn och påverkan från egen personal, inhyrda entreprenörer, samverkande parter och andra.

6.6.2 Inriktning

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. Den inre säkerheten och skydd mot insiders är primärt operatörernas eget ansvar. Operatörerna gör sina egna bedömningar på vilket sätt den inre säkerheten ska byggas upp och till vilken nivå. Det skydd som därmed skapas är avpassat till de krav som är kommersiellt motiverat och tar inte alltid nödvändigtvis hänsyn till samhällets behov av skydd för att klara fredstida kriser, svåra påfrestningar i fred eller vid höjd beredskap och krig. PTS kan vid

behov upphandla åtgärder som syftar till att stärka den inre säkerheten hos operatörerna utöver vad den normala säkerheten kräver.

6.6.3 Lämpliga åtgärder

6.6.3.1 Information

Genom information vill PTS öka medvetenheten hos operatörer och nätägare om inre säkerhet samt stimulera till att säkerhetshöjande åtgärder vidtas. För att uppnå god effekt bör man i första hand inrikta sig på att sprida kunskap bland dem inom företagen som har ett utpekat ansvar för säkerhet.

6.6.3.2 Säkerhetskontroller

Aktiva säkerhetskontroller och intrångsanalyser bidrar till att öka den inre säkerheten. Detta sker dels genom att brister i teknik och verksamhet identifieras och dels genom att medvetenheten om säkerhetsfrågorna ökas.

6.7 Fördjupat internationellt samarbete

Det internationella samarbetet för att öka säkerheten i elektroniska kommunikationer bör fördjupas. Det bör bland annat omfatta utveckling av standard och praxis, åtgärder för att förhindra eller försvåra skadebringande informationsoperationer, åtgärder för att underlätta gränsöverskridande samverkan vid fredstida kriser samt beredskap för samverkan inom ramen för internationell krishantering.

6.7.1 Syfte

De elektroniska kommunikationerna har kommit att bli allt mer gränsöverskridande till sin karaktär. Informationen kan sändas längs vägar som går utanför landets gränser även vid förbindelse mellan två inhemska punkter. Många operatörer är gränsöverskridande. Elektronisk kommunikation i Sverige påverkas i viss utsträckning av hur väl kommunikationssystemen skyddas och fungerar i andra länder. Även om man 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. Verksamhet för att höja säkerheten drivs inom ramen för internationellt verksamma organisationer, liksom utvecklingen av internationella normer.

Åtgärder inom detta område syftar till att stärka det internationella perspektivet på planering och utformning av beredskapen för extraordinära situationer inom elektroniska kommunikationer.

6.7.2 Inriktning

Det omfattande internationella samarbete under normala förhållanden som snabbt växer fram mellan såväl operatörer som reglerande myndigheter utgör en av delarna för att skapa säkra elektroniska kommunikationer också i extraordinära situationer.

PTS vill verka för att såväl myndigheten som enskilda aktörer skall få en god uppfattning om den internationella utvecklingen på säkerhetsområdet.

6.7.3 Lämpliga åtgärder

6.7.3.1 Informationsutbyte

Internationella kontakter ger goda möjligheter till utbyte av information runt arbete med att säkra de elektroniska kommunikationerna. Framförallt gäller detta erfarenheter av system och tekniska trender samt hot och konsekvenser för samhället. Informationsteknologiska hot utvecklas så snabbt att utbytet med andra länder ibland måste vara av operativ karaktär. För IT-incidentfunktionen (SITIC) är ett nära samarbete med motsvarande organ i andra länder av stor betydelse.

6.7.3.2 Standardisering

Många operatörer är idag gränsöverskridande och systemen växer ihop över nationsgränser. En harmonisering gällande tekniska säkerhetskrav och operativa säkerhetsnivåer är då viktig för att säkerställa att man inte får problem som sprider sig mellan länderna. Genom internationellt samarbete bör man utarbeta normer och krav som kan ställas på operatörer och nätägare inom elektroniska kommunikationer.

6.7.3.3 Tekniska varningssystem och barriärer

Internationellt samarbete för att utforma tekniska och organisatoriska varningssystem samt tekniska barriärer är viktigt. Denna typ av åtgärder reducerar risken för att störningar sprider sig mellan olika länder och i förlängningen påverkar de svenska elektroniska kommunikationerna.

6.7.3.4 Förbättrad förmåga till krishantering

Genom internationellt samarbete och planering förbättras möjligheterna till en effektiv krishantering. (Se även åtgärdsområdet 6.8 Förbättrad förmåga till krishantering inom elektroniska kommunikationer.)

6.8 Förbättrad förmåga till krishantering inom elektroniska kommunikationer

Trots alla förebyggande insatser går det inte att utesluta störningar och avbrott i de elektroniska kommunikationerna som kan få svåra konsekvenser för samhället. Åtgärder bör därför vidtas för att skapa en beredskap att lindra sådana konsekvenser och att snabbt avhjälpa störningar och avbrott. Det är viktigt att det finns tillgång till personal, reservutrustningar och mobila system som kan användas i svåra situationer och att genom planering och övning skapa en handlingsberedskap för att agera i kriser.

6.8.1 Syfte

Eftersom full säkerhet mot alla tänkbara hot aldrig kan uppnås kommer det att alltid finnas en risk för att de gemensamma satsningar som görs på funktionssäkerhet i de elektroniska kommunikationerna inte är tillräckliga för att undvika störningar och avbrott. Det är därför viktigt att allvarliga störningar eller avbrott i de elektroniska kommunikationerna snabbt kan avhjälpas. För detta behövs en effektiv krishantering som säkerställer att avbrotten blir korta och får en begränsad omfattning.

Åtgärderna inom detta område syftar till att förbättra förmågan till krishantering hos aktörerna inom elektronisk kommunikation.

6.8.2 Inriktning

PTS uppgift är inte att i ett akut skede leda krishanteringsarbetet utan att skapa förutsättningar för operatörerna att hantera kriser på bästa möjliga sätt.

Åtgärderna inom området skall stärka möjligheten att hantera störningar som trots förebyggande åtgärder ändå inträffar. Förmåga till krishantering utgör en väsentlig komplettering till de tidigare åtgärdsområdena som framför allt fokuserat på att undvika att störningar skall uppstå och leda till allvarliga konsekvenser som innebär kriser för samhället. Det är dock svårt att dra en skarp gräns mellan förebyggande och avhjälpande åtgärder varför en del aspekter på krishantering även diskuterats inom tidigare åtgärdsområden.

6.8.3 Lämpliga åtgärder

6.8.3.1 Övningar

Övningar och spel där krishanteringsförmågan utvärderas och övas är viktigt för att upprätthålla en god förmåga. Deltagare i dessa kan vara operatörer och nätägare men även representanter från elområdet och samhällsvikiga

verksamheter. Dessa övningar bör ske inom ramen för verksamheten i Samverkansområdet för teknisk infrastruktur.

6.8.3.2 Personal

Tillgången till kompetent personal är av avgörande betydelse för möjligheten att hantera krissituationer. Metoder och system för att larma och leda personal måste fungera även under störda förhållanden och behöver utvecklas. Möjligheterna att ta reservpersonal i anspråk vid extraordinära situationer bör ses över.

Det är viktigt att ta tillvara den kompetens som kan ha skapats genom deltagande i internationellt krishanteringsarbete såväl från myndigheter som näringslivet.

6.8.3.3 Reservutrustning

Reservutrustning och mobila system som kan användas vid krishantering är något som måste upphandlas innan en kris uppstår. Detta har även gjorts tidigare, men nya former för samarbete med operatörer och nätägare måste vidareutvecklas.

6.8.3.4 Internationellt samarbete

I och med att de elektroniska kommunikationerna liksom de flesta aktörerna inom området är gränsöverskridande är det viktigt med ett internationellt samarbete även när det gäller krishantering. I första hand gäller detta nordiskt och europeiskt samarbete.

6.9 Granskning av vilken funktionssäkerhet som uppnås i näten

PTS avser att följa upp vilken funktionssäkerhet som uppnås i näten för elektronisk kommunikation. Syftet är att lära av erfarenheter och skapa en grund för att styra och fördela resurser för att minska sårbarheten, öka robustheten och utveckla samverkan med andra inblandade parter.

6.9.1 Syfte

Det sker idag en mycket snabb teknisk utveckling inom området elektroniska kommunikationer. Det finns en mängd aktörer på området och många nya tillkommer, dessa aktörer konkurrerar på marknadsmässiga grunder, vilket medför att den offentliga insynen ibland är begränsad. Det finns därför ett behov av att kontinuerligt utvärdera vilken funktionssäkerhet som faktiskt uppnås i näten.

Syftet med detta är att möjliggöra en effektiv styrning och fördelning av PTS resurser, samt skapa underlag för samverkan med andra delar av samhället.

6.9.2 Inriktning

PTS har ett ansvar att hålla sig informerad och arbetar aktivt med detta.

PTS strävar efter att i det löpande arbetet och i de kontinuerliga kontakter man har med nätägare och operatörer bilda sig en övergripande uppfattning om den funktionssäkerhet som uppnås. Uppmärksammade brister utvärderas och analyseras.

PTS skall också aktivt ta initiativ till att granska funktionssäkerheten.

Ett område som behöver granskas är utvecklingen vad gäller utnyttjandet av elektronisk kommunikation. Speciellt viktigt ur ett risk- och sårbarhetsperspektiv är att granska konsekvenserna av den pågående integrationen av olika former för massmedial kommunikation.

Granskning och kunskapsuppbyggnad bör genomföras av PTS egen personal men för att nå djupare kan det vara nödvändigt att upphandla studier och forskning.

6.9.3 Lämpliga åtgärder

6.9.3.1 Praktiska tester

Genom praktiska tester av de elektroniska kommunikationerna kan PTS hålla sig informerad om deras uthållighet, tillgänglighet och tillförlitlighet. Tester kan vara tekniskt orienterade, men även inriktade på att testa rutiner och verksamhet.

6.9.3.2 Medverkan i uppföljningsstudier

Då större störningar inträffar medverkar PTS i de uppföljningsstudier och utredningar som genomförs för att få klarhet i vad som ledde fram till störningen och hur detta eventuellt hade kunnat undvikas. Vid behov initierar PTS fördjupade analyser eller vidtar andra åtgärder

6.9.3.3 Omvärldsbevakning

Omvärldsbevakning är mycket viktigt, såväl den tekniska som organisatoriska utvecklingen har på senare år varit mycket omfattande. I detta sammanhang kan man studera tekniska lösningar, arkitektur och uppbyggnad av system, systemens utnyttjande och hur flöden sker genom näten, men även hur olika operatörer och nätägare arbetar med funktionssäkerhet.

6.9.3.4 Granskning av säkerheten i den elektroniska mediedistributionen vid extraordinära situationer

Något som kräver speciell uppmärksamhet är att distributionen av public service TV sista ledet fram till hushållen ofta förmedlas via kabel-TV-nät.

6.9.3.5 Insamling och analys av störningsstatistik

En störningsstatistik av godtagbar kvalitet skulle kunna ge PTS underlag för bedömning av nätens sårbarhet och robusthet, vilket i sin tur skulle kunna hjälpa till vid prioritering av åtgärder. I första hand bör PTS verka för att operatörer samarbetar för att ta fram en godtagbar statistik. I andra hand kan PTS överväga metoder att föreskriva operatörer att redovisa störningsstatistik.

7 Grunder för prioritering av insatser

Riskerna för samhället av störda elektroniska kommunikationer i de extraordinära situationerna bestäms i någon mening av produkten av hot, teknisk sårbarhet och konsekvenser för samhället. Svårast är de fall när extraordinära men ändå rimligt tänkbara situationer kan medföra hot som systemen för elektronisk kommunikation är påtagligt sårbara för samtidigt som de störningar som kan uppkomma medför stora konsekvenser för samhällets funktion. Satsningar på åtgärder för att öka de elektroniska kommunikationernas motståndskraft vid svåra påfrestningar på samhället i fred, höjd beredskap och krig skall därför i första hand göras när:

- De kommersiella drivkrafterna inte skapar tillräcklig säkerhet i de extraordinära situationerna
- Åtgärderna motverkar eller minskar konsekvenser för viktiga samhällsfunktioner om kommunikationssystemen utsätts för hot som bedöms vara rimliga i de extraordinära situationerna
- Åtgärderna bedöms vara kostnadseffektiva

Åtgärder bör också väljas så att en balans uppnås mellan förebyggande åtgärder, som minskar risken att störningar skall uppkomma eller lindrar deras karaktär, och avhjälpande åtgärder, som medger att situationen kan hanteras och kapacitet kan återuppbyggas om störningar trots allt skulle inträffa. Åtgärder bör också vidtas för att fortlöpande kunna lära av erfarenheter och förbättra säkerheten för framtiden.

Litteratur

Litteraturförteckningen är indelad i förarbeten och styrdokument samt rapporter och publikationer. Förarbeten redovisas i kronologisk ordning med det senaste dokumentet sist. Övriga kategorier är sorterade i bokstavsordning efter titel.

Förarbeten och styrdokument

Prop. 2001/02:10 Fortsatt förnyelse av totalförsvaret

Prop. 2001/02:158 Samhällets säkerhet och beredskap

Regleringsbrev för budgetåret 2002 avseende Post- och telestyrelsen m.m. inom utgiftsområde 22 Kommunikationer (rskr 1999/2000:256 och 2001/02:90 och 125)

Planeringsinriktning för samhällets krisberedskap 2004, Krisberedskapsmyndigheten

Prop. 2002/03:110 Lag om elektronisk kommunikation, m.m.

Försvarsberedningens säkerhetspolitiska rapport ”Säkrare grannskap – osäker värld” (Ds 2003:8)

Rapporter och publikationer

Telekommunikationernas sårbarhet och risker för samhället. Konsultrapport insänd till regeringen av Post- och Telestyrelsen med skrivelsen *Delrapport avseende PTS strategi för att minska konsekvenser av svåra påfrestningar på de elektroniska kommunikationssystemen*, diarienummer 02-12281

Är Internet i Sverige robust? Internets uppbyggnad och användning. Internets beroende av funktioner utomlands. Post- och telestyrelsen PTS-ER-2003:1

Bilaga 1 – Telekommunikationernas sårbarhet och risker för samhället

Innehåll

1	Sammanfattning av rapporten.....	44
2	Hoten.....	44
3	Den tekniska sårbarheten.....	45
4	Risker för samhället vid bortfall av elektronisk kommunikation.....	46
5	Samlad värdering.....	47
6	Fortsatt arbete.....	49

PTS lämnade den 30 september 2002 en delredovisning av ett uppdrag från regeringen att för telekommunikationerna redovisa en strategi för hur arbetet skall bedrivas med åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och med att öka beredskapen inför höjd beredskap och krig. Därvid insändes rapporten Telekommunikationernas sårbarhet och risker för samhället författad av två konsulter Göran Franzén, BDO Consulting Group Stockholm AB och Svante Barck-Holst, Totalförsvarets forskningsinstitut.

1 Sammanfattning av rapporten

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

2 Hoten

Som svåra påfrestningar på samhället benämns situationer där det uppstår 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 ökar risken 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 avsiktliga 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. Hot kan också utövas med informationsteknologiska 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.

3 Den tekniska sårbarheten

Rapporten diskuterar den tekniska sårbarheten hos fasta telenät, mobila telenät, nät för datakommunikation, IT-infrastruktur med hög överföringskapacitet samt de elektroniska kommunikationernas beroende av el. Rapporten 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 beroende av el för att fungera. Avbrott i elförsörjningen på upp till ett par timmar klaras normalt då de flesta noder i telenäten är försedda med batteribackup. Centrala noder klarar sig normalt längre då de utöver batteribackup ofta har reservkraft i form dieselgeneratorer. Ett av de vanligaste problemen anges av operatörerna dock vara elavbrott.

4 Risker för samhället vid bortfall av elektronisk kommunikation

Elektronisk kommunikation är idag en viktig funktion för i stort sett alla samhällsområden. En fullständig eller samlad bild är svår för att inte säga omöjlig att sammanställa. Det kan dock konstateras 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 faktureringsystem som är direkt beroende av fungerande telekommunikationer.

Sveriges betalningssystem är mycket beroende av fungerande tele- och datakommunikationer. De olika aktörerna i betalningssystemet överför varje dag stora belopp mellan varandra. Detta datautbyte sker till största delen via fiber som hyrs av teleoperatörerna. Likaså sker en stor del av betalningarna i handeln numera via betalkortsterminaler 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, länsstyrelser, kommuner och landsting, polisen, sjukvården, elförsörjningen och media. Vid höjd beredskap och krig är totalförsvarets elektroniska kommunikationer av avgörande betydelse.

5 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 elektroniska kommunikationer 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 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 bilden 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. Även om försiktighetsåtgärder företas för att förhindra intrång i styrdäten är det tveksamt 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.

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 i stor utsträckning är nedgrävda. Där antalet fysiskt åtskilda vägar för informationsflödet är begränsat 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 för access 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 en yttre sabotör som vill orsaka störningar genom att klippa av kablar eller förstöra knutpunkter. Det är därför för säkerheten väsentligt 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 beroendet mellan systemen för elförsörjning och telekommunikation. Väderstörningar drabbar ofta både elförsörjning och telekommunikationer samtidigt 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 extraordinära situationer.

De informationsteknologiska 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 internationellt problem. Elektronisk kommunikation i Sverige påverkas 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 till delar också vara beroende av ett internationellt samarbete.

Under arbetets gång framkom att det fanns anledning att vid en genomgång av telekommunikationernas sårbarhet och risker för samhället också ta med distribution av ljudradio och TV. Detta har dock inte gjorts i denna delrapport.

6 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, att öva och utveckla möjligheter till krishantering.

Bilaga 2 – Sårbarhet i distributionen av radio och TV

Innehåll

1	Bakgrund	50
2	Hot.....	50
3	System och sårbarheter	51
3.1	Aktörer.....	51
3.2	Tekniska system.....	52
3.3	Sårbarheter.....	54
3.3.1	Systemnivå.....	54
3.3.2	Objektnivå	55
4	Risker för samhället	56
5	Bedömning	57

1 Bakgrund

PTS lämnade med rapporten Telekommunikationernas sårbarhet och risker för samhället den 30 september 2002 en delredovisning av ett uppdrag från regeringen 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. En insikt i delredovisningen var att det förelåg ett behov av att inkludera distribution av ljudradio och TV vid en genomgång av sårbarheten i systemen för elektronisk kommunikation och risker för samhället.

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 allt mer integrerade. Vid svåra påfrestningar i fred och vid höjd beredskap och krig spelar tillgång till snabb och tillförlitlig information från media en stor roll.

Denna bilaga kompletterar den ovan nämnda rapporten med en analys av sårbarheterna i systemen för distribution av radio och TV. Syftet är att bidra med utökad underlag till den strategi för att tillgodose skyddet av elektroniska kommunikationer vid svåra påfrestningar på samhället i fred, höjd beredskap och krig som redovisas i denna rapport.

2 Hot

En hotklassificering redovisades i Telekommunikationernas sårbarhet och risker för samhället. Många av hoten som diskuterades i den rapporten gäller även för systemen för distribution av radio och TV.

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 informationsteknologiska medel.

Systemen för distribution av radio och TV ger möjlighet att rikta sig med information till stora grupper på en gång. I krissituationer är systemen viktiga för att sprida information som underlättar krishanteringsarbetet. För en angripare som vill sprida förvirring kan det då vara intressant att störa distributionen.

I stället för att störa eller förstöra systemen kan en angripare eller terrorist inrikta sig på att utnyttja distributionssystemen för egna syften, som ett led i informationskrigföring eller i syfte att väcka uppmärksamhet för sin fråga.

3 System och sårbarheter

Först presenteras de viktigaste aktörerna för marksänd radio och TV i Sverige. Därefter beskrivs den teknik och de system som används. Slutligen diskuteras systemens sårbarheter.

3.1 Aktörer

Sveriges Television AB (SVT) och Sveriges Radio AB (SR) har till uppgift att bedriva TV- respektive ljudradioverksamhet i allmänhetens tjänst. Tillsammans med Sveriges Utbildningsradio AB (UR) utgör de svensk public service. SVT:s och SR:s sändningstillstånd kräver att de använder analog sändningsteknik för sändning av ljud och bild, även om SVT och SR dessutom får sända med digital teknik. Det är vidare uttalat av regeringen att SVT och SR skall köpa utsändningstjänster för analoga marksändningar av Teracom AB (Sändningstillstånd för Sveriges Television AB, Kulturdepartementet dec 2001 och Sändningstillstånd för Sveriges Radio AB, Kulturdepartementet dec 2001).

Teracom är ett aktieföretag helägt av staten. Teracom's huvudverksamhet är distribution av radio och TV. Frågor som rör Teracom har inom Regeringskansliet tidigare hanterats av Kulturdepartementet men sedan 1 januari 2003 ligger ansvaret på Näringsdepartementet.

Enligt sändningstillstånden måste public service-bolagen anlita Teracom för utsändning. De tjänster som omfattas är analog utsändning av radio och TV för public service-bolagen samt TV4. Teracom's övriga verksamhet är konkurrensutsatt och prissättningen av tjänsterna är marknadsanpassad. Denna del av verksamheten domineras av Teracom's roll som nätoperatör då man tillhandahåller transmissionskapacitet till sina kunder. Tjänsterna omfattar även digital utsändning av radio och TV. Dessutom erbjuder Teracom service och

inplaceringstjänster, vilket innebär att kunderna hyr plats i Teracoms hus och master (Teracom årsredovisning 2001).

SVT, SR, UR och Teracom har specifika krav på sig från regeringen vid höjd beredskap och vid svåra påfrestningar på samhället i fred. En hög säkerhet och uthållighet i distributionen av radio och TV skall eftersträvas. Bolagen åläggs att årligen beredskapsplanlägga för sina verksamheter under höjd beredskap och vid svåra påfrestningar för samhället i fred. Bolagen skall samråda sinsemellan, med Styrelsen för psykologiskt försvar (SPF) samt med andra berörda myndigheter i beredskapsfrågor. SPF har fått i uppgift att vara samrådsorgan i frågor om beredskap på medieområdet (Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap).

3.2 Tekniska system

Public service programbolag sänder radio- och TV-signaler som distribueras ut i landet genom Teracoms stamnät, där ingår rikstäckande nät för TV samt fyra rikstäckande FM-nät för SR och UR. Teracoms nät av markbundna sändare når ut till 99,8 % av Sveriges befolkning.

Kaknästornet i Stockholm fungerar som huvudknutpunkt för Teracoms olika nät. Vid Kaknästornet övervakas alla rikstäckande TV- och radiosändningar och där sker den operativa styrningen av näten. De färdiga riksprogrammen kommer till Kaknäs från programbolagen. Från Kaknäs distribueras de ut via länknätet till sändarstationer ute i landet. Länknätet används också för att förmedla programinslag till programbolagen (s.k. kontribution) samt till tele- och datatrafik för programbolag och övriga kunder.

I Sverige finns 54 större sändarstationer som sänder ut radio och TV till merparten av Sveriges befolkning genom Teracoms analoga marknät. Stationerna är anläggningar som innehåller erforderliga programförbindelser, sändarutrustningar, reservkraftaggregat samt antensystem mm. Större sändarstationer har oftast en cirka 300 m hög mast av fackverkskonstruktion försedd med sändarantennor för i första hand radio och TV men även för mobiltelefoni, kommunikationsradio mm. Stationerna har också radiolänkutrustning och ingår i det landstäckande radiolänknätet.

Distributionen mellan sändarstationerna kan ske genom Teracoms markbundna analoga nät på tre olika sätt vidare ut i landet, antingen via radiolänk, i kabel med fiberoptik eller genom relämatning.

I dagsläget sker distributionen från programbolagen i regel via radiolänknätet till sändarna. En radiolänksändning innebär en överföring från en punkt till en annan och därför koncentreras sändningen mot den avsedda mottagaren. Signalerna utgår från sändarstationers parabol och beskriver radiolänklinjer där avståndet mellan sändare och mottagare är cirka 50 km. Radiolänklinjerna

kombineras därför i flera led av radiolänkstationer för att täcka merparten av Sverige.

Teracoms radiolänknät har på vissa sträckor ersatts med hyrd bandbredd i fiberoptisk kabel.

Möjlighet finns även att distribuera signaler via relämatning. Detta är enbart en reservåtgärd som kopplas in automatiskt om den ordinarie distributionen inte fungerar. Relämatningen innebär att en station tar emot sändningarna från en grannstation med en vanlig radio- eller TV-mottagare och återutsänder dessa på sin egen frekvens.

Sveriges kuperade terräng gör att de större sändarstationerna inte når ut till samtliga hushåll. Teracom har därför mindre obemannade stationer som genom relämatning kompletterar utsändningen för att avhjälpa täckningsbrister. Dessa så kallade slavsändare saknar egna programförbindelser, det vill säga de tar endast emot signaler från större stationer och återutsänder dem lokalt på andra frekvenskanaler.

Sista ledet i distributionen av radio och TV är normalt att signalerna sänds till abonnenterna från Teracoms rundstrålande radio- och TV-sändare. Rundstrålande sändare kräver ingen specifik mottagare utan utsänder signaler över hela ytan till många hushåll.

Distribution och utsändning kan också ske via satellit. Satellitsändningar kan tas emot på ett flertal sätt. Sändarstationerna kan ta emot satellitsändningar och återutsända dem via marknätet, hushållen kan ta in satellitsändningar direkt med egna parabol- eller så kan satellitsändningar tas emot av någon kabel-TV-anläggning som sänder signalen vidare i kabel till hushållen. Satellitkommunikationens sårbarheter beskrivs närmare i Telekommunikationens sårbarhet och risker för samhället.

Kabel-TV-näten fungerar som ett alternativt sista distributionsled mellan de markbundna sändningsnäten respektive satellitsändningarna och konsumenterna. Detta är ett vanligt förekommande alternativ till att ta emot marksändningarna direkt via rundradio.

Lokala radiosändningar över geografiskt begränsade områden kan delas in i privat lokalradio som drivs av kommersiella bolag och närradio som är öppen för lokala organisationer. Teracom handhar en stor del av dessa sändningar.

Informationssystemet VMA (Viktigt meddelande till allmänheten) används för att nå ut till berörda människor med information och varningar i allvarliga akuta situationer. Statens räddningsverk har överenskommelser gällande utsändningen av varningsmeddelandet med SR, SVT, TV4 samt Radioutgivarföreningen som företräder de privata lokalradiostationerna. Överenskommelsen innebär att programbolagen är skyldiga att sända myndighetsmeddelanden kostnadsfritt i nödsituationer (Regeringens skrivelse

2000/2001:52 Beredskapen mot svåra påfrestningar mot samhället i fred). SR har det operativa ansvaret för VMA som begärs av räddningsledning eller annan behörig och förmedlas till SR via SOS-centralerna. SR förmedlar sedan informationen vidare till SVT, TV4 samt kommersiella radiokanaler.

Den statliga Digital-TV-kommittén föreslog 2001 att de analoga TV-sändningarna skulle avvecklas och släckas år 2007. Riksdagen skulle ha tagit ställning till förslaget under hösten 2002, men ärendets proposition är försenad och har ännu inte lagts. Med digital teknik kan överföringskapaciteten ökas fyra till fem gånger i jämförelse med dagens analoga distributionsätt. För att kunna ta del av digitala utsändningar krävs konverteringsutrustning hos konsumenten.

Distribution av radio och TV sker idag även till en viss del via Internet. Bedömningen är att denna form av distribution kommer att öka.

3.3 Sårbarheter

Sårbarheterna diskuteras först på en övergripande systemnivå och sedan behandlas enskilda komponenter på objektnivå.

3.3.1 Systemnivå

Teracoms rikstäckande distributionsnät bedöms generellt som robust. Avsiktliga angrepp och sabotagehandlingar utgör det dominerande hotet. Systemets sårbarhet för slumpmässiga hot såsom felhandlingar, tekniska fel och extremt väder får anses låg.

De enskilda objekten är relativt lätta för en angripare att slå ut men det finns god tillgång till reservmöjligheter och flexibilitet i systemet. Det bedöms därför som svårt att åstadkomma långvariga avbrott i distribution och sändning av radio och TV. För detta krävs resursstarka angripare med möjlighet till avancerade sabotage eller enklare angrepp i stora mängder.

Det allvarigaste avsiktliga hotet är att flera närliggande sändarstationer slås ut vid en precisionsinsats. Det drabbar främst utsändningen över det aktuella begränsade området men kan även riskera att störa möjligheterna till vidare distribution via radiolänk eller relämatning.

På systemnivå är det viktigt med flexibilitet och att enstaka objekt inte får för stor betydelse. Centralisering av funktioner och integrering av teknik gör att bortfall får större konsekvenser. I Teracoms nät utgör Kaknästornet och de större sändarstationerna sårbara knutpunkter där utslagning kan ge stor effekt. De större sändarstationerna ingår som komponenter i både radiolänknätet och relämatningsnätet. Stationerna innehåller dessutom annan teknik för elektronisk kommunikation i data och telenät.

Om ordinarie distribution via radiolänk och kabel förhindras finns fortfarande möjlighet till reläomtagning. En FM/TV-station kan då agera slavstation och ta emot en närliggande stations program och återutsända dessa. Omkoppling till sådan relämatning sker automatiskt vid behov.

I högtrafikerade områden av Teracoms nät finns omfattande dubbeltäckning. Dubbeltäckning innebär att stationerna är så tätt belägna att mer än en sändarstation täcker ett visst område, så att hushållen fortfarande kan ta emot sändningarna även om den närmaste sändaren inte fungerar.

Vad gäller sårbarheten mot informationsteknologiska hot påminner situationen gällande radio- och TV-distribution starkt om de förhållanden som råder vid övrig elektronisk kommunikation. De finns beskrivna i Telekommunikationers sårbarhet och risker för samhället.

Den inre säkerhetens betydelse ökar då nätstyrning centraliseras. Undvikande av insiders blir avgörande för säkerheten. Teracom har specialtillstånd att utföra registerkontroll på personal i nyckelpositioner för den inre säkerheten samt besluta om placering i säkerhetsklass 2 och 3. Teracoms medarbetare behöver i regel ha tillgång till mycket information och styrfunktioner i sitt dagliga arbete vilket förhindrar möjligheten att begränsa tillgången till insyn och styrning för medarbetarna.

SVT, SR och UR får statliga bidrag till sitt beredskapsarbete och köper för dessa medel bl.a. beredskapsåtgärder från Teracom. TV4 och övriga kommersiella programbolag däremot har inga säkerhetsmässiga krav på sig från statsmakten och erhåller därmed inga bidrag. Det finns heller inga ställda krav på kabel-TV-nätens distribution vilket kan upplevas som en säkerhetsmässig lucka i ett i övrigt robust system. Detta visade sig exempelvis i Uppsala 2 oktober 2002 då Telias kabel-TV-nät com hem slogs ut. Abonnenter med endast com hem kunde då inte se SVT1, SVT2, TV4 eller några andra kabelkanaler.

3.3.2 Objektnivå

Även på objektnivå finns tillräcklig redundans för att Teracoms distributionsnät skall uppfattas som robust avseende slumpmässiga hot. De enskilda objekten är dock relativt lätta för en angripare att slå ut.

Sändarstationerna har visst fysiskt skydd samt tillträdesskydd och de större stationerna är skyddsobjekt men inga stationer är placerade i bergrum. De är täckningsmässigt strategiskt belägna fullt synligt med höga master. Det enklaste sättet för en angripare att bekämpa en station är att förstöra kablarna som går inuti masterna.

Radiolänkstationer bedöms även som känsliga för angrepp med elektromagnetisk puls (HPM) eftersom antenner inte går att skydda. Systemet kan bli utsatt för förstöring från relativt stora avstånd i klart väder då parabolen fungerar som mottagarantenn för HPM-strålningen (Sårbarhet i de civila telekommunikationerna av Ulf Petterson, Petter Wulff, Georg Fischer, Försvarets forskningsanstalt (Numera Totalförsvarets forskningsinstitut) FOA-R—99-01221-240—SE oktober 1999 ISSN 1104-9154). Kvalificerade angrepp med HPM-vapen kräver dock mycket resursstarka angripare.

Om en station förstörs eller på annat sätt slås ut kan sändningen i regel återupptas inom ett par timmar. Det finns Outside Broadcasting-grupper (OB-grupper) med fordonsburen radiolänkutrustning, mastfordon med antennmateriel samt reservkraftaggregat som kan skickas ut som komplement för att ersätta bruten radiolänktransmission. Det finns också transportabla FM- och TV-reservsändare som kan ersätta skadade radiolänkstationer eller bidra vid upprättande av tillfälliga produktionsplatser. Inom Teracom finns katastrofplanering och förteckningar över var all reservmateriel finns.

Kaknästornet, de större sändarstationerna och Teracoms radiolänkstationer är försedda med stationära reservkraftaggregat avsedda i första hand för SVT och SR. Dessutom förfogar Teracom över transportabla elverk. Vid ett elavbrott bör därför distribution och utsändning av SR:s och SVT:s program kunna fortsätta utan störningar för större delen av landet. I en del områden där slavsändare saknar reservkraft kan störningar uppstå. För hushåll är elberoendet för mottagningen av TV den stora svårigheten.

Som alternativ till Kaknästornet finns en reservoperatörsplats samt motsvarande funktioner i skyddade utrymmen (Teracoms beredskapsplan för 2002-2004).

Fiberoptiska nät medför kabelberoende och kablar är sårbara i det avseendet att de går att klippa av. Kabelns höga kapacitet innebär att många funktioner leds i samma kabel vilket ökar konsekvenserna vid avbrott. Näten har dock i regel inbyggd redundans och skydd för de viktigaste noderna.

4 Risker för samhället

Dagens samhälle är beroende av snabb och tillförlitlig information. Såväl enskilda som beslutsfattare inom företag och myndigheter hämtar beslutsunderlag från radio och TV. Avbrott i detta informationsflöde skapar osäkerhet och kan leda till beslut som får konsekvenser av ekonomisk eller annan art.

Behovet av information är större i en krissituation. Distributionssystemen för radio och TV är i detta fall nödvändiga för att förmedla direkta varningar, myndighetsinformation samt fri och oberoende nyhetsinformation och opinionsbildning. På så sätt kan skador begränsas och osäkerheten minskas. Radio och TV fyller även en viktig funktion i att avlasta trycket på andra

kommunikationskanaler. I en akut kris kan andra kanaler för elektronisk kommunikation snabbt blockeras av oroliga och nyfikna som vill informera sig. Dessa kanaler är samtidigt viktiga för att leda arbetet med krishantering.

5 Bedömning

Den generella bedömningen är att systemen för distribution av radio och TV är robusta.

Något som speciellt kräver uppmärksamhet är att distributionen av public service TV sista ledet fram till hushållen ofta förmedlas via kabel-TV-nät.

Möjligheter som finns att ytterligare stärka robustheten i systemen för elektronisk kommunikation genom att utnyttja och i viss mån samordna de olika systemen bör beaktas. Exempelvis bör det undersökas om den reservkraftförsörjning som finns för Teracoms master i större utsträckning även kan utnyttjas av mobiltelefoninätens radiobasstationer.

En ökad teknikintegration har lett till att gränserna för vilka system som används för att förmedla elektronisk information delvis har suddats ut. Detta exemplifieras av att Teracoms radiolänknät utnyttjas för annat än distribution av radio och TV samt att radio och TV idag, i ökande utsträckning, finns tillgängligt via Internet.

Sammanfattningsvis bör den ökade integrationen av olika system för elektronisk kommunikation motivera ett nära samarbete mellan de myndigheter och företag som är verksamma inom området.

Litteratur

Proposition 2001/02:158 Samhällets säkerhet och beredskap

Skrivelse 2000/2001:52 Beredskapen mot svåra påfrestningar mot samhället i fred

Sändningstillstånd för Sveriges Television AB, Kulturdepartementet dec 2001

Sändningstillstånd för Sveriges Radio AB, Kulturdepartementet dec 2001

Teracoms beredskapsplan för 2002-2004

Teracom årsredovisning 2001

Planeringsinriktning för samhällets krisberedskap 2004, Krisberedskapsmyndigheten

Telekommunikationernas sårbarhet och risker för samhället. Konsultrapport insänd till regeringen av Post- och Telestyrelsen med skrivelsen *Delrapport avseende PTS strategi för att minska konsekvenser av svåra påfrestningar på de elektroniska kommunikationssystemen*, diarienummer 02-12281

Massmediers beredskap och SPF:s roll inom samhällets säkerhet och beredskap. Mats Ekeblom, Ekeblom Konsult AB, 2002-11-18.

Planeringsunderlag för säkerhets- och beredskapsåtgärder för Styrelsen för psykologiskt försvar 2004, Styrelsen för Psykologiskt Försvar.

Sårbarhet i de civila telekommunikationerna. Ulf Petterson, Petter Wulff, Georg Fischer, Försvarets forskningsanstalt, FOA-R—99-01221-240—SE oktober 1999 ISSN 1104-9154

Svåra påfrestningar – Säkerheten inom el, tele, rundradio vid ett nytt totalförsvarsperspektiv, Christina Frost, Staffan Molin, Ulf Pettersson, Per Ånäs, FOA-R-96-00257-1.2-SE juni 1996 ISSN 1104-9154

Beredskapsåtgärder inom rundradiodistributionen, Ulf Pettersson, Peter Wallström, Per Ånäs, Försvarets forskningsanstalt, FOA-R—97-00451-240—SE november 1995 ISSN 1104-9154

Teracoms beredskap, Ulf Pettersson, Peter Wallström, Per Ånäs, Försvarets forskningsanstalt, FOA-R—97-00452-240—SE november 1995 ISSN 1104-9154