

DATUM
24 april 2006

RAPPORTNUMMER
PTS-ER-2006:19
ISSN 1650-9862

DIARIENR
06-7972

Robusta elektroniska kommunikationer

Strategi för åren 2006-2008

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. PTS redovisade nämnda regeringsuppdrag i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2003-2005”, PTS-ER-2003:13, 2003-03-31.

Denna strategi utgör en fortsättning av tidigare strategi inom ramen för verksamhetsområde Det civila försvaret och verksamhetsområde Svåra påfrestningar och sträcker sig mellan åren 2006-2008

I det omfattande beredskapsarbete som genomförts har vissa tidigare mål som eftersträvats för att vidmakthålla och öka robustheten i de elektroniska kommunikationerna uppnåtts. Den snabba teknikutvecklingen i sektorn gör det däremot nödvändigt att vidareutveckla det ständigt pågående säkerhetsarbetet om nuvarande robusthetsnivå skall kunna vidmakthållas och förbättras.

Den starkt ökande användningen av olika former av elektronisk kommunikation, inte minst datakommunikation och Internets utbredning, gör samhället alltmer beroende av fungerande elektroniska kommunikationer. De tekniska system som används för kommunikation blir alltmer komplexa och sammanlänkade. De integrerar i växande utsträckning ljud, bild och data i digital form i samma kanaler. Elberoendet är stort. Utslagning av vitala delar av de elektroniska kommunikationerna kan ge stora konsekvenser för samhället.

Förändringarna av hot, teknik och samhällets beroende gör det nödvändigt att ständigt utveckla arbetet med att öka robustheten i de elektroniska kommunikationerna. Sverige är i hög grad beroende av effektiva och robusta elektroniska kommunikationer. Sverige har också ett internationellt ansvar då de svenska elektroniska kommunikationssystemen många gånger utgör delar i det globala elektroniska kommunikationssystemen. Tillförlitlighet, uthållighet och tillgänglighet behöver tillgodoses inte minst när samhället utsätts för svåra påfrestningar. Åtgärderna måste utformas så att de svarar mot dagens hot och vad vi kan förutse för framtiden, kopplat till den snabba tekniska utvecklingen på området och de alltför samhällsviktiga tjänster som är beroende av säkert fungerande kommunikationer.

Strategin som presenteras ger en inriktning av det arbete som bedrivs och avses bedrivas under de närmaste åren för att tillgodose behovet av tillförlitlighet, uthållighet och tillgänglighet hos de elektroniska kommunikationerna vid kriser och extraordinära händelser.

Marianne Treschow

Generaldirektör

Innehåll

Sammanfattning	9
1 Inledning.....	11
1.1 PTS är central förvaltningsmyndighet med sektorsansvar inom inområdena post och elektronisk kommunikation	11
1.2 Strategin är en uppdatering av en tidigare strategi på området.....	11
1.3 Utgångspunkter för strategin med tolkning av begreppen i uppdraget	12
1.3.1 Strategin omfattar alla typer av elektronisk kommunikation	12
1.3.2 Strategin är myndighetens inriktning för att tillgodose robusthetsbehoven.....	12
1.3.3 Förklaringar till begreppen svåra påfrestningar i fred, höjd beredskap och krig.....	12
1.3.4 Hot, sårbarheter och åtgärder.....	13
1.4 Metod för arbetet med strategin	13
1.5 Strategins struktur	14
2 Politiska och organisatoriska utgångspunkter för robustare elektronisk kommunikation	15
2.1 Behoven i samhället har förändrats där den tekniska infrastrukturen utgör en del i den gemensamma sårbarheten.....	15
2.2 Samhällets behov tillgodoses genom en helhetssyn på samhällets resurser.....	15
2.3 Samhällets struktur för krishantering bygger på ett sektors- och områdesansvar baserat på flera principer.....	16
3 Arbetet med robustare elektroniska kommunikationer har bedrivits länge och utvecklats utifrån samhällets behov	17
3.1 Tidigare satsningar på robusthet har i stor utsträckning koncentrerats mot totalförsvarets behov av fungerande telekommunikationer	17
3.2 Dagens behov med en föränderlig värld ställer krav på en strategi som löpande kan tillgodose robustheten i de elektroniska kommunikationerna	17
4 Målen för robusta elektroniska kommunikationer	19
4.1 De elektroniska kommunikationerna ska ha sådan kapacitet att viktiga samhällsfunktioner kan upprätthållas.....	19
4.2 De elektroniska kommunikationerna skall medverka till att säkerställa livsnödvändiga funktioner och möjliggöra ett effektivt försvar.....	20
5 Samverkan.....	21
6 Åtgärdsområden	22
6.1 Stimulera till ett ökat användaransvar inom elektroniska kommunikationer	23
6.1.1 Syftet är att stimulera samhällsviktiga verksamheter att skapa en god robusthet i sina elektroniska kommunikationer.....	23
6.1.2 Inriktning är att samhällsviktiga verksamheter själva skall vidta åtgärder för att säkerställa tillräcklig robusthet.....	23
6.1.3 Exempel på åtgärder.....	24
6.1.3.1 Tillhandahålla information och rådgivning.....	24
6.1.3.2 Medverka i uppföljningsstudier.....	24
6.2 Öka redundans och flexibilitet i nätverk.....	25
6.2.1 Syftet är att göra näten för elektronisk kommunikation mer robusta	25
6.2.2 Inriktningen är att öka redundans och omkopplingsmöjligheter	25

6.2.3	Exempel på åtgärder	26
6.2.3.1	Utveckla möjligheter till prioritering.....	26
6.2.3.2	Tillföra extra noder.....	27
6.2.3.3	Skapa redundanta förbindelser	27
6.2.3.4	Samutnyttja nät vid extraordinära situationer.....	27
6.2.3.5	Genomföra tester och övningar.....	27
6.3	Förbättra skyddet mot både fysiska och elektromagnetiska hot	28
6.3.1	Syftet är att minska risken för att kritiska delar av de elektroniska kommunikationerna slås ut	28
6.3.2	Inriktningtningen är att vidmakthålla och utveckla skyddet mot nya krav	28
6.3.3	Exempel på åtgärder	29
6.3.3.1	Förstärka det tekniska skalskyddet.....	29
6.4	Öka kunskapen om informationssäkerhet	30
6.4.1	Syftet är att öka kunskapen om informationssäkerhet	30
6.4.2	Inriktning är att varna, informera och ge stöd om informationssäkerhet och incidenter.....	30
6.4.3	Exempel på åtgärder	30
6.4.3.1	Bidra till höjd säkerhetsnivå.....	30
6.4.3.2	Genomföra tekniska tester	30
6.4.3.3	Bidra till utvecklingen av standarder.....	31
6.5	Verka för robustare elförsörjning för de elektroniska kommunikationerna och fördjupa samarbetet mellan el- och teleområdena	32
6.5.1	Syftet är att skapa robustare elförsörjning för de elektroniska kommunikationerna och robustare elektroniska kommunikationer för elförsörjningen.....	32
6.5.2	Inriktningen är att skapa gemensamma strukturer för informationsutbyte och utveckla formerna för hur nyttja reservkraft så effektivt som möjligt.....	32
6.5.3	Exempel på åtgärder	33
6.5.3.1	Investera i robustare elförsörjning	33
6.5.3.2	Utföra gemensamma tester och övningar	33
6.6	Utveckla samverkan.....	34
6.6.1	Syftet är att förbättra samarbetsformer och rutiner	34
6.6.2	Inriktningen är att genomföra övningar och seminarier.....	34
6.6.3	Exempel på åtgärder	34
6.6.3.1	Fortsätta med nationell telesamverkan	34
6.6.3.2	Samverka mellan sektorerna el och elektronisk kommunikation	35
6.6.3.3	Genomföra regionala el- och telesamverkansseminarier mellan sektorsansvariga och områdesansvariga aktörer	35
6.7	Fördjupa det internationella samarbete	36
6.7.1	Syftet är att utveckla det internationella perspektivet i planering och utformning av beredskapen för extraordinära situationer	36
6.7.2	Inriktningen är att aktivt delta i internationella forum och utveckla bilaterala kontakter med andra nationer	36
6.7.3	Exempel på åtgärder	36
6.7.3.1	Utbyta information	36
6.7.3.2	Delta i standardiseringsarbete.....	37
6.7.3.3	Delta i utvecklingen av tekniska varningssystem	37
6.7.3.4	Förbättra förmågan till krishantering.....	37
6.8	Förbättra förmågan till krishantering inom elektroniska kommunikationer.....	38

6.8.1	Syftet är att förbättra förmågan till krishantering inom sektorn elektronisk kommunikation	38
6.8.2	Inriktningen är att genomföra övningar och införskaffa reservutrustning	38
6.8.3	Exempel på åtgärder	38
6.8.3.1	Genomföra övningar	38
6.8.3.2	Utbilda personal	38
6.8.3.3	Införskaffa reservutrustning.....	39
6.8.3.4	Utveckla internationellt samarbete	39
6.9	Öka robustheten i näten	40
6.9.1	Syftet är att effektivisera resursutnyttjandet och utveckla samverkan med andra delar i samhället	40
6.9.2	Inriktningen är att kontinuerligt utveckla kunskaperna och förståelsen för den komplexa utveckling som sker	40
6.9.3	Exempel på åtgärder	40
6.9.3.1	Utföra praktiska tester	40
6.9.3.2	Medverka i uppföljningsstudier.....	40
7	Grunder för prioritering av insatser	41

Sammanfattning

Regeringen gav med regleringsbrevet 2002 Post- och telestyrelsen (PTS) 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 avsåg åren 2003 t.o.m. 2005. Uppdraget redovisades den 31 mars 2003 till regeringen. Denna strategi, för åren 2006-2008, är en vidareutveckling av den tidigare strategin.

Föreliggande dokument redovisar PTS strategi inom ramen för verksamhetsområde Det civila försvaret och verksamhetsområde Svåra påfrestningar.

PTS redovisar mål för robusta elektroniska kommunikationer vid extraordinära händelser och svåra påfrestningar på samhället.

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 robustheten i de elektroniska kommunikationerna vid extraordinära händelser.

Därefter redovisas ett antal olika åtgärdsområden som PTS anser angelägna för insatser. För varje sådant område redovisas syfte, inriktning och exempel på 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. Öka kunskapen om informationssäkerhet
5. Robustare elförsörjning för de elektroniska kommunikationerna och fördjupat samarbete mellan el- och teleområdena
6. Utveckla samverkan
7. Fördjupat internationellt samarbete
8. Förbättrad förmåga till krishantering inom elektroniska kommunikationer
9. Ökad robusthet i näten

Avslutningsvis redovisar PTS grunder för prioritering av insatser.

1 Inledning

1.1 PTS är central förvaltningsmyndighet med sektorsansvar inom områdena post och elektronisk kommunikation

Post- och telestyrelsen är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom områdena post och elektronisk kommunikation.

PTS har såsom sektorsmyndighet ett ansvar för att samhällets behov av elektroniska kommunikationer 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 Strategin är en uppdatering av en tidigare strategi på området

Den tidigare strategin sträckte sig mellan 2003 – 2005 och benämndes ”Strategi för robusta elektroniska kommunikationer” (PTS-ER-2003:13).

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.”

Uppdraget redovisades den 31 mars 2003 till regeringen i form av en rapport benämnd ”Strategi för robusta elektroniska kommunikationer” (PTS-ER-2003:13).

Denna strategi för åren 2006-2008 är en uppdatering och vidareutveckling av den tidigare strategin.

1.3 Utgångspunkter för strategin med tolkning av begreppen i uppdraget

1.3.1 Strategin omfattar alla typer av elektronisk kommunikation

I och med tillkomsten av lagen (2003:389) om elektronisk kommunikation har det tidigare använda begreppet telekommunikationer utgått. Istället används begreppet 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 kopparledning, 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 sårbarheter är det därför nödvändigt att se de alltmer konvergerande formerna av elektronisk kommunikation i ett helhetsperspektiv.

1.3.2 Strategin är myndighetens inriktning för att tillgodose robusthetsbehoven

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 sektorsansvarig myndighet och hur sektorn genom privatoffentlig samverkan kan verka för att tillgodose tillförlitlighet, uthållighet och tillgänglighet hos de elektroniska kommunikationerna vid extraordinära händelser och svåra påfrestningar.

Strategin anger principer för arbetet med att minska sårbarheten och öka robustheten hos de elektroniska kommunikationerna. Principerna skall tillämpas under åren 2006 – 2008. De konkreta åtgärderna kan däremot 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 robusta elektroniska kommunikationer. Strategin utgör 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 och exempel på insatser och grunder för prioritering. Viktiga sådana åtgärdsområden utgörs av de i nämnda regeringsuppdrag 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 Förklaringar till 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 Hot,, sårbarheter och åtgärder

Hot, och sårbarheter för de elektroniska kommunikationerna kan tolkas i vid mening. Strategin har valt att beskriva dessa i tre steg. De utgör

1. tänkbara hot mot de elektroniska kommunikationerna vid extraordinära händelser, och svåra påfrestningar på samhället i fred,
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 mindre kriser, extraordinära händelser, 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 genomförts av PTS, enheten för samhällsättagande. 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 stormen Gudrun januari 2005, det stora teleavbrottet i södra Sverige 2003, 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.

1.5 Strategins struktur

Strategin 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 extraordinära händelser och svåra påfrestningar. Denna text finns med framför allt för att ge dem som skall tillämpa strategin för robusta elektroniska kommunikationer en lättillgänglig bakgrund om hur samhällets beredskap och säkerhet hanteras i stort.

I kapitel 3 redovisas kortfattat tidigare satsningar på robusthetsarbete i de elektroniska kommunikationerna. Dessa satsningar relateras sedan till dagens behov.

I kapitel 4 redovisas ett till dagens förhållanden anpassat mål för robusta elektroniska kommunikationer vid extraordinära händelser och svåra påfrestningar. 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 robusthetsarbetet i de elektroniska kommunikationerna bör bedrivas. Vad som redovisas är en inriktning av kompletterande säkerhetshöjande 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.

2 Politiska och organisatoriska utgångspunkter för robustare elektronisk kommunikation

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 ”Förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap” och Krisberedskapsmyndighetens planeringsunderlag ”Samhällets krisberedskap Planerad verksamhet 2006”. 0249/2005 PTS har också noterat de successiva förändringarna som indikeras genom Försvarsberedningens rapport ”En strategi för Sveriges säkerhet”, (Ds 2006:1). Inriktningar spårbara i propositionen ”Samverkan vid kris – för ett säkrare samhälle” (prop. 2005/06:133) har också inarbetats i strategin.

2.1 Behoven i samhället har förändrats där den tekniska infrastrukturen utgör en del i den gemensamma sårbarheten

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 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 understryker betydelsen av att minska samhällets sårbarhet. 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, elektroniska kommunikationer och ekonomiska system uppnå en del av de effekter på samhället och civilbefolkningen som det tidigare krävdes militära maktmedel för att uppnå.

2.2 Samhällets behov tillgodoses genom en helhetssyn på samhällets resurser

Samhällets samlade behov av säkerhet och beredskap tillgodoses genom en helhetssyn på samhällets resurser. Det innebär att utgångspunkten för krishanteringsarbetet 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 sitt fredstida skydd och sin fredstida förmåga att hantera normalt förekommande

störningar och påfrestningar. Därigenom skapas en grundläggande förmåga att tillgodose behovet av säkerhet och beredskap.

- Staten svarar för att komplettera denna grundläggande förmåga med åtgärder för att hantera hela hotskalan från allvarliga fredstida kriser till höjd beredskap och krig. Därigenom skapas en förmåga att möta allvarliga hot och påfrestningar samt en handlingsfrihet att kunna anpassa förmågan på medellång och lång sikt.

2.3 Samhällets struktur för krishantering bygger på ett sektors- och områdesansvar baserat på flera principer

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. Det är:

- 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 överensstämma i fred, kris och krig. Närhetsprincipen innebär i sin tur att en kris skall hanteras så nära den aktuella krisen som möjligt.

3 Arbetet med robustare elektroniska kommunikationer har bedrivits länge och utvecklats utifrån samhällets behov

3.1 Tidigare satsningar på robusthet har i stor utsträckning koncentrerats mot totalförsvarets behov av fungerande telekommunikationer

Sedan länge har det varit av 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 precisionsstyrda 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 1990-talet har investeringar genomförts för att förlägga viktiga växlar och centrala delar av transmissionsnät och styrsystem i skyddade utrymmen i form av berggrum. Detta gällde inledningsvis främst TeliaSoneras nät men har efterhand utvidgats till att omfatta flera operatörer. Idag finns ett stort antal operatörer som har bedömts vara samhällsviktiga förlagda i dessa berggrum. De skyddade utrymmena utgör därmed viktiga knutpunkter för de elektroniska kommunikationerna.

Även andra åtgärder har vidtagits för att minska sårbarheten och öka robustheten exempelvis förstärkning av reservkraft och ökad redundans. Redundans kan beskrivas som fler förbindelser som skapar flera maskor i näten vilket därmed ger möjligheter att koppla förbi skadade delar av näten.

Under de senaste åren har arbetet främst koncentrerats till att förstärka reservkraftsförsörjningen, förbättra redundansen och utveckla krishanteringsförmåga och samverkansformer.

Det finns således en värdefull grund att bygga vidare på, samtidigt som det pågående arbetet måste anpassas utifrån den snabba teknik- och marknadsutvecklingen som pågår inom de elektroniska kommunikationerna.

3.2 Dagens behov med en föränderlig värld ställer krav på en strategi som löpande kan tillgodose robustheten i de elektroniska kommunikationerna

Ett invasionshot mot Sverige ter sig inte möjligt under minst en tioårsperiod. Samtidigt har andra typer av hot från kriminella grupper, terrorister och icke-

demokratiska stater blivit mer påtagliga. Samhället kan också utsättas för svåra påfrestningar genom andra extraordinära omständigheter.

Den tekniska utvecklingen inom området elektronisk kommunikation går mycket snabbt vilket bl.a. medfört ett utökat utbud och därmed ökat beroende av de elektroniska kommunikationerna. Centralisering och fjärrstyrning av trafiken gör såväl lokal, regional, nationell som internationell elektronisk kommunikation alltmer beroende av fungerande förbindelser till några få noder. Noder som ibland är placerade utanför rikets gränser.

De ständiga förändringarna gör sammantaget att det finns behov av en strategi som är anpassad för att löpande kunna tillgodose robustheten i de elektroniska kommunikationerna.

4 Målen för robusta elektroniska kommunikationer

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 för att nå målet/målen är att bibehålla och öka robustheten i de elektroniska kommunikationerna.

Lagen om elektronisk kommunikation anger följande mål för sektorn elektronisk kommunikation.

”Enskilda och myndigheter skall få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet.

Syftet skall uppnås främst genom att konkurrensen och den internationella harmoniseringen på området främjas. Samhällsomfattande tjänster skall dock alltid finnas tillgängliga på för alla likvärdiga villkor i hela landet till överkomliga priser.”

I såväl privata som statliga aktörers nät finns inbyggt en grundläggande nivå vad gäller säkerhet och uthållighet. Denna förmåga bestäms utifrån kommersiella överväganden samt reglering av marknaden enligt lagen (2003:389) om elektronisk kommunikation. Denna förmåga kan kompletteras dels genom privatoffentlig samverkan med delad finansiering dels med statliga beslut med statligt finansierade åtgärder.

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

4.1 De elektroniska kommunikationerna ska ha sådan kapacitet att viktiga samhällsfunktioner kan upprätthållas

Vid svåra påfrestningar på samhället i fred skall de elektroniska kommunikationerna ha sådan kapacitet 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. Allmänhetens behov av information och möjligheter till kommunikation för att kunna hantera uppkomna krissituationer måste alltid tillmätas stor vikt.

4.2 De elektroniska kommunikationerna skall medverka till att säkerställa livsnödvändiga funktioner och möjliggöra ett effektivt försvar

Tänkbara hot vid höjd beredskap och krig är 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 de elektroniska kommunikationerna så att de kan motstå dessa.

Vid hotande väpnat angrepp eller i krig skall de elektroniska kommunikationerna 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.

5 Samverkan

Att öka robustheten i de elektroniska kommunikationerna och indirekt öka tillgången till elektronisk kommunikation i händelse av en kris kräver omfattande förebyggande och direkt samverkan såväl mellan operatörerna och myndigheten inom sektorn elektronisk kommunikation som med näringslivsaktörer inom andra sektorer, centrala och regional myndigheter samt kommuner.

Samverkan ska utgå från de former för elektronisk kommunikation som under normala förhållanden och fri konkurrens växer fram i samhället.

Samverkan ska utveckla rutiner för samverkan och öka förståelsen för olika aktörers verksamheter och ansvarsområden.

Inom sektorn elektronisk kommunikation skall staten genom privatoffentlig samverkan med de enskilda aktörerna med utnyttjande av ekonomiska incitament och överenskommelser öka robustheten i de elektroniska kommunikationerna. Informationsutbyte, gemensamma krisövningar, gemensamma system och praktiska försök utgör viktiga medel för koordinering och samverkan.

Vid upphandling av kompletterande robusthetshöjande åtgärder skall strävan vara att genomföra dessa i samband med utbyggnad, nybyggnation och reinvestering inom systemen för elektronisk kommunikation.

Åtgärder för att öka robustheten för att möta kriser bidrar ofta till ökad säkerhet även under normala förhållanden. Sådana åtgärder har också ett visst kommersiellt värde även om det inte är tillräckligt för att de skall komma till stånd på rent kommersiella grunder. När sådana åtgärder vidtas skall ambitionen vara att genom privatoffentlig samverkan nå uppgörelser om samfinansiering mellan staten och enskilda aktörer.

6 Åtgärdsområden

Nedan presenteras ett antal områden som PTS anser det angeläget att genomföra insatser inom för att öka robustheten 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 i dagens säkerhetspolitiska läge, svaga punkter i systemen, samhällets ökade beroende av elektroniska kommunikationer, behovet av också mjuka kunskapsorienterade insatser och att utöver förebyggande insatser också satsa på förmåga att hantera såväl stora som mindre störningar.

Vissa åtgärder inom ett antal av dessa områden är relativt billiga, men är personellt resurskrävande. De bedöms ge hög effekt om än med begränsad varaktighet. Upprepade insatser är därför nödvändiga. Exempel på sådana åtgärder är information, samverkan, samarbete, internationellt samarbete och övningar.

Andra åtgärder kräver mer omfattande investeringar. Exempel på sådana åtgärder är utbyggnad av redundans, reservförsörjning och vidmakthållande av centrala noder.

6.1 Stimulera till ett ökat användaransvar inom elektroniska kommunikationer

Samhällsviktiga funktioner skall uppmärksammas på att vidta åtgärder för att skapa god säkerhet i sina egna elektroniska kommunikationer.

6.1.1 Syftet är att stimulera samhällsviktiga verksamheter att skapa en god robusthet i sina elektroniska kommunikationer

Utifrån den egna verksamheten varierar användarnas krav på funktionssäkerhet i de elektroniska kommunikationerna. Vissa användare klarar utan större olägenheter relativt långa avbrott och betydande kvalitetssänkningar i de tjänster som erbjuds. Andra användare har små eller inga toleranser.

Med stor sannolikhet går det att göra en bedömning att skydd mot alla tänkbara hot aldrig kan garanteras. Vissa användare kommer alltid att ha högre krav på funktionssäkerhet än den generella robusthet som marknaden erbjuder. Det är inte en realistisk ambition att anpassa den ”generella” robustheten i de elektroniska kommunikationerna efter användare med de högsta kraven på funktionssäkerhet. Det är därför viktigt att användare har en bild av de egna behoven och tydligt kan beskriva dessa vid en upphandling.

Användarens kan gardera sig mot de risker som föreligger. Det kan göras genom att i avtal med operatörer ställa krav på tillgänglighet, genom att anskaffa reservalternativ, genom att anskaffa lokalt skydd mot såväl dataintrång som fysiskt intrång etc.

Detta åtgärdsområde syftar till att stimulera samhällsviktiga verksamheter att utifrån sina behov skapa en god 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 extraordinära händelser, påfrestningar på samhället i fred, höjd beredskap och krig.

6.1.2 Inriktning är att samhällsviktiga verksamheter själva skall vidta åtgärder för att säkerställa tillräcklig robusthet

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 möjlighet som PTS utnyttjar i detta sammanhang är att informera om olika åtgärder som användare kan vidta för att öka robustheten.

Åtgärderna inom detta område omfattar information och rådgivning.

6.1.3 Exempel på åtgärder

6.1.3.1 *Tillhandahålla information och rådgivning*

För vissa användare kan det vara alltför kostsamt att hålla egen kunskap hur man skall säkerställa sina elektroniska kommunikationer. 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.

Det kan även ske behovsstyrt. En del i arbetet innebär att PTS är kontaktpunkt för all samhällsviktig verksamhet i frågor som rör elektronisk kommunikation.

6.1.3.2 *Medverka i uppföljningsstudier*

Erfarenheter, som visar hur större störningar drabbar användare, bör spridas till andra intressenter såsom områdesansvariga myndigheter och 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 Ökad robusthet i näten.)

6.2 Öka 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 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 kunna skapa.

Fortsatta studier avseende möjligheter att prioritera trafik i de elektroniska kommunikationerna ska genomföras.

Försvarsmaktens behov av tillgång till de publika näten skall uppmärksammas.

6.2.1 Syftet är att göra näten för elektronisk kommunikation mer robusta

En konsekvens av att nätfunktioner och tjänster fortlöpande centraliseras och att näten i allt större utsträckning fjärrövervakas och fjärrstyrs innebär att delar av landet kan bli avskurna vid skador i näten. Förbindelseavbrott med centrala delar i näten kan innebära att även lokala kommunikationer inte kan upprätthållas. Risken är särskilt stor för norra Sverige, Gotland och delar av landet med begränsat befolkningsunderlag.

Detta åtgärdsområde syftar i huvudsak till att göra näten för de elektroniska kommunikationerna mer robusta genom att minska risken för avbrott vid kriser. Risken för samtidigt förekommande störningar på flera ställen är då särskilt stor.

6.2.2 Inriktningen är att öka redundans och omkopplingsmöjligheter

Åtgärderna inom detta område skall inriktas mot att dels öka möjlighet till redundans i näten och dels skapa förutsättningar för att kunna utnyttja de omkopplingsmöjligheter som de tekniska systemen kan mede. Inriktningen på åtgärderna är att minska risken för avbrott vid kriser då risken för samtidigt förekommande störningar på flera ställen är särskilt stor.

Åtgärderna inom detta område bör beakta att i en krissituation är de samhällsviktiga aktörerna ofta beroende av fungerande elektroniska kommunikationer för att kunna hantera krisen. Detta ställer krav på att funktionen elektronisk kommunikation kan upprätthållas trots störningar i samhället.

Investeringar kommer att erfordras för att öka redundansen och flexibiliteten i näten efterhand som dessa utvecklas så att även mer omfattande och avsiktliga störningar kan hanteras. 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 övergripande 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 operatörers nät.

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

Vid satsningar på åtgärder för att förbättra redundans och flexibilitet i näten för elektronisk kommunikation skall följande fyra förhållanden 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. Vissa delar av landet är exempelvis mer utsatta för extremt väder, vissa platser kan vara mer intressanta som mål för sabotage och terrorism.
- **Sårbara funktioner.** Vissa funktioner 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 störningar och avbrott.

6.2.3 Exempel på åtgärder

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

6.2.3.1 Utveckla 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. PTS förbereder en första rapport till regeringen 3Q 2006.

6.2.3.2 *Tillföra extra noder*

Genom att tillföra extra noder som avlastar eller speglar andra noder reduceras effekten av att noder faller bort. Det går även att investera i noder som kan flyttas till en plats där det anses behövas.

Idag finns ett stort antal nätägare. Genom att tillföra hopkopplingspunkter och länkar mellan dessa nät går det att skapa ökad redundans.

6.2.3.3 *Skapa redundanta förbindelser*

Fler förbindelser ger flera maskor i näten och ger möjlighet att koppla förbi skadade delar i näten.

Ur ett nationellt robusthetsperspektiv är det viktigt att följa upp så att nya fiberstråk inte läggs längs redan existerande sträckningar, utan att man väljer andra vägar för att få fler fysiskt åtskilda maskor i näten.

Investeringar i extra noder eller redundanta förbindelser kan genomföras efter gemensamma analyser av nätägare och PTS. Den privatoffentliga samverkan måste därför hållas ständigt aktuell för att PTS och nätägarna skall kunna vidta åtgärder på det mest kostnadseffektiva sättet.

6.2.3.4 *Samutnyttja nät vid extraordinära situationer*

Det finns idag ett flertal nät för elektroniska kommunikationer vilka ägs av olika aktörer. Att nyttja flera nät ger teoretiska möjligheter till ökad redundans. Det är angeläget att löpande följa utvecklingen och utreda vilka tekniska och ekonomiska möjligheter som står till buds och vilka överenskommelser mellan operatörerna som krävs, för att snabbt skall kunna samutnyttja nät om skador i näten uppstår.

6.2.3.5 *Genomföra tester och övningar*

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

6.3 Förbättra skyddet mot både fysiska och elektromagnetiska hot

De viktigaste delarna som för närvarande existerar av näten 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 som inte är förlagda i bergtrum behöver också skyddas mot skador på grund av olyckor och avsiktlig skadegörelse.

6.3.1 Syftet är att minska risken för att kritiska delar av de elektroniska kommunikationerna slås ut

De elektroniska kommunikationerna utgörs av tekniska system, placerade på platser som ofta är relativt lätt fysiskt åtkomliga, de har dessutom en geografisk utbredning i landet. 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 Inriktningningen är att vidmakthålla och utveckla skyddet mot nya krav

De centrala noderna i elektronisk kommunikation har under senare år givits ett bra skydd genom förläggning i bergtrum. Fortsatta åtgärder skall 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 också uppmärksammas. Övriga viktiga noder som idag inte finns i bergtrum bör skyddas från skador som kan uppkomma på grund av svåra olyckor eller skadegörelse.

Liksom för åtgärdsområdet 6.2 skall följande fyra förhållanden beaktas:

- 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 dubbleras. Utspridning och många möjligheter till vägval i maskformiga nät kan också ge säkra elektroniska kommunikationer utöver ett bra skydd för centrala noder i hierarkiska nät.

6.3.3 Exempel på åtgärder

6.3.3.1 Förstärka det tekniska skalskyddet

Utrustning av stor betydelse kan vid behov ges ett förstärkt tekniskt skalskydd..
Exempel på åtgärder kan vara kompletterande insatser för att ge viktiga noder skydd i bergrum samt upphandling av skydd mot elektriska och elektromagnetiska hot.

6.4 Öka kunskapen om informationssäkerhet

PTS skall i sitt arbete med informationssäkerhet och i samverkan med andra berörda aktörer i samhället beakta angrepp mot de elektroniska kommunikationerna 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 Syftet är att öka kunskapen om informationssäkerhet

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.

6.4.2 Inriktning är att varna, informera och ge stöd om informationssäkerhet och incidenter

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.

Inom detta åtgärdsområde förutser PTS ett behov av insatser för att öka kunskapen om informationsangrepp.

6.4.3 Exempel på åtgärder

6.4.3.1 Bidra till höjd säkerhetsnivå

PTS sprider information som bidrar till ett ökat skydd mot informationsangrepp. Genom informationsspridning till operatörer och nätägare avser PTS att sprida kunskap och uppmuntra till samarbete i dessa frågor.

6.4.3.2 Genomföra tekniska tester

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

6.4.3.3 Bidra till utvecklingen av standarder

Där så är möjligt avser PTS att bidra till utveckling av standarder gällande exempelvis teknisk utrustning, riktlinjer för incidentrapportering, kryptering, certifiering och säkerhetsnivåer gällande skydd mot informationsangrepp.

6.5 Verka för robustare elförsörjning för de elektroniska kommunikationerna och fördjupa samarbetet mellan el- och teleområdena

De elektroniska kommunikationerna är beroende av en fungerande elförsörjning samtidigt som samhället har behov av 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 för att minska konsekvenserna av det ömsesidiga beroendet vid avbrott.

6.5.1 Syftet är att skapa robustare elförsörjning för de elektroniska kommunikationerna och robustare elektroniska kommunikationer för elförsörjningen

De senaste årens elavbrott exemplifierat i stormen Gudrun januari 2005, teleavbrottet i Uppsala den 2 oktober 2002, tunnelbränderna i Kista 2001 och 2002 visar att det inte är möjligt att säkerställa en helt störningsfri elförsörjning samtidigt som långvariga elavbrott utgör ett av de allvarligaste hoten mot de elektroniska kommunikationerna.

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.

PTS och Svenska Kraftnät (SvK) leder flera samarbetsprojekt mellan de bägge sektorerna. Ett fördjupat samarbete mellan el- och teleområdena är ett viktigt medel för att minska sårbarheten mot störningar inom bägge sektorerna.

Åtgärder inom detta område syftar till att skapa en robustare elförsörjning för de elektroniska kommunikationerna och robustare elektroniska kommunikationer för elförsörjningen.

6.5.2 Inriktningen är att skapa gemensamma strukturer för informationsutbyte och utveckla formerna för hur nyttja reservkraft så effektivt som möjligt

PTS samarbetar med Svenska Kraftnät, Statens Energimyndighet och andra aktörer på el- och telemarknaden för att minska risken för störningar. En struktur för ömsesidigt informations- och erfarenhetsutbyte bör utvecklas för att förbättra och snabba upp kontakten mellan representanter för el- och teleområdena.

Samarbetet mellan el- och teleområdena bör leda till samordnade åtgärder för att höja beredskapen inom såväl el som elektroniska kommunikationer. Målet är att kunna utnyttja respektive systems styrkor och minimera dess svagheter. Denna samverkan bör även innefatta planering för krishantering.

Behovet av elektroniska kommunikationer som finns inom elförsörjningen i samband med kraftiga störningar i elförsörjningen beaktas särskilt.

PTS bedömer att behovet av investeringar kommer att öka för att uppnå en robustare elförsörjning för de elektroniska kommunikationerna.

6.5.3 Exempel på åtgärder

6.5.3.1 Investera i robustare elförsörjning

Satsningar på lösningar för reservkraft bör när så är möjligt ske i samarbete med representanter för elområdet och teleoperatörerna.

Där gemensamma intressen finns från såväl el- som det elektronisk kommunikationsområdet avser PTS att utöka samarbetet avseende åtgärder som reducerar konsekvenserna av det ömsesidiga beroendet.

PTS och SvK leder ett regionalt samarbetsprojekt där berörda elnätsägare och operatörer elektronisk kommunikation deltar. Syftet är att identifiera det ömsesidiga beroendet på regional och lokal nivå och efterhand vidta konkreta åtgärder för att öka robustheten.

6.5.3.2 Utföra 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 Utveckla samverkan

Samverkan mellan olika aktörer såväl branschföreträdare, sektorsansvariga myndigheter som områdesansvariga aktörer är en förutsättning för effektiv krishantering.

Samverkan måste vara förberedd innan en kris uppstår om en effektiv krishantering skall kunna genomföras.

6.6.1 Syftet är att förbättra samarbetsformer och rutiner

De senaste årens avbrott visar att det inte är möjligt att säkerställa en helt störningsfri elektronisk kommunikation till samhället.

Det är många aktörer såväl inom krishanteringssystemet som utanför som påverkas när det uppstår störningar i de elektroniska kommunikationerna. Många aktörer är beroende av information från sektorn elektronisk kommunikation för att vid dessa händelser kunna vidta relevanta åtgärder. Samtidigt är sektorns aktörer beroende av andra aktörers information och åtgärder för att kunna vidta relevanta åtgärder, som leder till minskade avbrottstider.

PTS och Svenska Kraftnät leder flera samarbetsprojekt dels mellan de bägge sektorerna och dels med andra sektorer, andra myndigheter och områdesansvariga aktörer i syfte att öka informationsutbytet.

Åtgärder inom detta område syftar till att skapa förberedda och fungerande samarbetsformer och rutiner.

6.6.2 Inriktningen är att genomföra övningar och seminarier

PTS samarbetar med SvK, operatörer, branschföreträdare, centrala myndigheter, områdesansvariga myndigheter och kommuner och flera andra aktörer för att utveckla en struktur för ömsesidigt informations- och erfarenhetsutbyte. Samarbetet bör leda till att åtgärder skall kunna vidtas koordinerat för största effekt såväl för operatörer som områdesansvariga aktörer.

Målet är att genom att nyttja förberedda rutiner och upparbetade kontaktnät effektivt utbyta information i syfte att få största möjliga effekt av gemensamma insatser.

6.6.3 Exempel på åtgärder

6.6.3.1 Fortsätta med nationell telesamverkan

PTS, TeliaSonera, 3, Teracom, TDC Song, Vodafone, Tele2, Telenor, Stokab, Banverket, Stadsnätsföreningen och Försvarsmakten har tillsammans bildat en nationell telesamverkansgrupp. Gruppen är en funktion som kan träda i kraft vid

svåra påfrestningar i syfte att minimera avbrottstider inom de elektroniska kommunikationerna. Gruppen utgör också stommen för att utveckla samarbetet med elsektorn.

6.6.3.2 Samverka mellan sektorerna el och elektronisk kommunikation

Elsektorn har delat in Sverige i sju elsamverkansområden. Kopplat till dessa finns sju elsamverkansledningar. En elsamverkansledning startar sin verksamhet i samband med en allvarlig störning inom elförsörjningen. Flera övningar har genomförts och ytterligare kommer att genomföras för att etablera samarbete mellan den nationella telesamverkansgruppen och elsamverkansledningarna.

6.6.3.3 Genomföra regionala el- och telesamverkansseminarier mellan sektorsansvariga och områdesansvariga aktörer

PTS, SvK, elnätsägare, nätägare elektronisk kommunikation och länsstyrelser avser genomföra ett antal regionala el- och telesamverkansseminarier i landet. Förutom redan uppräknade deltagare kommer representanter för kommuner, Sveriges Radio, SoS Alarm och landsting att delta. Syftet är att utveckla förståelse för respektive aktörs ansvarsområde och utveckla krishanteringssamarbetet.

6.7 Fördjupa det internationella 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 Syftet är att utveckla det internationella perspektivet i planering och utformning av beredskapen för extraordinära situationer

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 extraordinära händelser, svåra påfrestningar på samhället i fred, höjd beredskap och krig, kommer säkerheten också att vara beroende av 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 utveckla det internationella perspektivet på planering och utformning av beredskapen för extraordinära situationer inom elektroniska kommunikationer.

6.7.2 Inriktningen är att aktivt delta i internationella forum och utveckla bilaterala kontakter med andra nationer

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.

PTS deltar i ett stort antal internationella organ och hänvisar till PTS årsredovisning för en mer detaljerad beskrivning av de olika organen.

6.7.3 Exempel på åtgärder

6.7.3.1 Utbyta information

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 (SIITC) är ett nära samarbete med motsvarande organ i andra länder av stor betydelse.

6.7.3.2 Delta i standardiseringsarbete

Många operatörer är idag gränsöverskridande och systemen växer ihop över nationsgränser. En harmonisering gällande tekniska säkerhetskrav och operativa säkerhetsnivåer är en ständigt pågående process.

6.7.3.3 Delta i utvecklingen av tekniska varningssystem

Internationellt samarbete för att utforma tekniska och organisatoriska varningssystem 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 Förbättra förmågan till krishantering

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

6.8 Förbättra förmågan 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 snabbt avhjälpa störningar och avbrott. Det måste finnas tillgång till personal, reservutrustningar och mobila system som kan användas i svåra situationer och att genom planering och övning skapa en handlingsberedskap för att kunna agera i kriser.

6.8.1 Syftet är att förbättra förmågan till krishantering inom sektorn elektronisk kommunikation

Det kommer alltid att finnas risker för störningar och avbrott i de elektroniska kommunikationerna. Allvarliga störningar eller avbrott i de elektroniska kommunikationerna måste snabbt kunna avhjälpas. För detta behövs en effektiv krishantering som säkerställer att avbrotten blir så korta som möjligt och får en begränsad omfattning.

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

6.8.2 Inriktningen är att genomföra övningar och införskaffa reservutrustning

PTS och operatörerna arbetar förebyggande för att skapa förutsättningar för operatörerna att kunna hantera kriser på bästa möjliga sätt. I de akuta situationerna är det alltid operatörerna som leder krishanteringsarbetet.

Åtgärderna inom området syftar till att stärka möjligheten att hantera störningar som trots förebyggande åtgärder ändå inträffar.

6.8.3 Exempel på åtgärder

6.8.3.1 Genomföra övningar

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

6.8.3.2 Utbilda 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.

6.8.3.3 *Införskaffa reservutrustning*

Reservutrustning och mobila system som kan användas vid krishantering är något som måste upphandlas innan en kris uppstår. Former för samarbete med operatörer och elnätsägare måste vidareutvecklas.

6.8.3.4 *Utveckla 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 Öka robustheten i näten

Robustheten i näten för elektronisk kommunikation måste ständigt följas upp. Syftet är att lära av erfarenheter och skapa en grund för att styra och fördela tillgängliga resurser effektivt för att minska sårbarheten, öka robustheten och utveckla samverkan med andra inblandade parter.

6.9.1 Syftet är att effektivisera resursutnyttjandet och utveckla samverkan med andra delar i samhället

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 insynen är begränsad. Det finns därför ett behov av att kontinuerligt utvärdera vilken robusthet som faktiskt uppnås i näten.

Syftet med detta är ett effektivt resursutnyttjande samt skapa underlag för samverkan med andra delar i samhället.

6.9.2 Inriktningen är att kontinuerligt utveckla kunskaperna och förståelsen för den komplexa utveckling som sker

I det löpande arbetet och i de kontinuerliga kontakterna mellan PTS och operatörerna måste PTS bilda sig en övergripande uppfattning om den robusthet som uppnås.

6.9.3 Exempel på åtgärder

6.9.3.1 Utföra 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 Medverka i uppföljningsstudier

Då större störningar inträffar skall PTS delta i uppföljningsstudier och utredningar som genomförs för att få klarhet i vad som ledde fram till störningen. Vid behov initierar PTS fördjupade analyser eller vidtar andra åtgärder

7 Grunder för prioritering av insatser

Satsningar på åtgärder för att öka de elektroniska kommunikationernas motståndskraft vid extraordinära händelser, svåra påfrestningar på samhället skall i första hand göras när:

- De kommersiella drivkrafterna inte skapar tillräcklig robusthet 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 mest 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.

