

Robust elektronisk kommunikation

Strategi för åren 2009-2011



Robust elektronisk kommunikation

Rapportnummer

PTS-ER-2009:25

Diarienummer

09-7583

ISSN

1650-9862

Författare

Jonny Nilsson
Anders Rafting
Eva Ekenberg

Post- och telestyrelsen

Box 5398
102 49 Stockholm
08-678 55 00
pts@pts.se
www.pts.se

Förord

Regeringen gav i regleringsbrevet för 2002 Post- och telestyrelsen (PTS) ett uppdrag att redovisa en strategi för hur arbetet ska bedrivas när det gäller åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och för att öka beredskapen inför höjd beredskap och krig. PTS redovisade nämnda regeringsuppdrag i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2003-2005”, PTS-ER-2003:13, 2003-03-31 och i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2006-2008”, PTS-ER-2006:19, 2006-04-24

Strategin 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 elektronisk kommunikation vid kriser och extraordinära händelser.

Denna rapport är en uppdatering av tidigare strategi inom ramen för utgiftsområde 6 ”Försvar och samhällets krisberedskap” och avser perioden 2009 till 2011.

Marianne Treschow
Generaldirektör

Innehåll

Förord	3
Sammanfattning	6
1 Inledning	7
1.1 PTS är central förvaltningsmyndighet med sektorsansvar inom områdena post och elektronisk kommunikation	7
1.2 Strategin är en uppdatering och vidareutveckling av tidigare strategier på området	7
1.3 Utgångspunkter för strategin med tolkning av begreppen i uppdraget	8
1.3.1 <i>Strategin omfattar allmänt tillgänglig elektronisk kommunikation</i>	8
1.3.2 <i>Strategin är myndighetens inriktning för att tillgodose behoven av robust elektronisk kommunikation</i>	8
1.3.3 <i>Förklaring till allvarliga hot och påfrestningar i fred, höjd beredskap och krig</i>	9
1.3.4 <i>Hot, sårbarheter och åtgärder</i>	9
1.4 Metod för arbetet med strategin	10
1.5 Strategins struktur	10
2 Politiska och organisatoriska utgångspunkter för robust elektronisk kommunikation	12
2.1 Viktigt att minska sårbarheten i samhällets tekniska infrastruktur	12
2.2 Samhällets behov tillgodoses genom en helhetssyn på samhällets resurser	12
2.3 Samhällets struktur för krishantering bygger på ett sektors- och områdesansvar baserat på flera principer	14
3 Infrastrukturen för elektronisk kommunikation och hot, sårbarheter samt beroenden	15
3.1 Modell av elektroniska kommunikationsnät	15
3.2 "Internetteknik" används i allt större utsträckning	15
3.3 Ökad sårbarhet till följd av centralisering och konvergerande teknik	16
3.3.1 <i>Ökad centralisering och fjärrstyrning av trafiken ökar beroendet av fungerande förbindelser</i>	16
3.3.2 <i>Konvergensen och komplexa system kan öka sårbarheterna</i>	16
3.3.3 <i>Ny GSM-standard bidrar ytterligare till konvergens mot IP</i>	16
3.4 Beroendet av externt kontrollerade resurser	17
3.4.1 <i>Immateriella resurser för trafik baserad på Internetteknik</i>	17
3.4.2 <i>Beroendet av intern och extern DNS-tjänst</i>	18
3.5 Ny version av Internet Protocol (IP) kommer att införas vid sidan av det nuvarande	19
4 Arbetet med robust elektronisk kommunikation görs utifrån samhällets behov	20
4.1 Tidigare satsningar på robusthet i elektronisk kommunikation inriktades främst mot totalförsvarets behov	20
4.2 Åtgärder krävs för att säkerställa tillförlitligheten till elektronisk kommunikation	20
4.3 Fortsatta åtgärder för ökad robusthet och krishanteringsförmåga i såväl krig som fred	21
4.3.1 <i>Samverkan i krishantering genom den Nationella Telesamverkansgruppen (NTSG)</i>	22
4.3.2 <i>GLU - ett system för gemensam lägesuppfattning av störningar och avbrott</i>	22
4.3.3 <i>Alternativ överföring av korrekt spårbar tid</i>	23
4.3.4 <i>Stärkt robusthet för funktionen för IP-samtrafik</i>	23
4.3.5 <i>Behov av ökad tillgänglighet och tillförlitlighet till DNS</i>	24
5 Målen för robust elektronisk kommunikation	25
5.1 Elektronisk kommunikation ska ha sådan kapacitet att viktiga samhällsfunktioner kan upprätthållas även vid kriser	26

5.2	Elektronisk kommunikation ska medverka till att säkerställa livsnödvändiga funktioner och möjliggöra ett effektivt försvar	27
6	Samverkan	28
7	Åtgärdsområden	29
7.1	Stimulera till ett ökat användaransvar inom elektronisk kommunikation	29
7.1.1	<i>Syftet är att stimulera samhällsviktiga verksamheter att skapa en god robusthet för sin elektroniska kommunikation</i>	29
7.1.2	<i>Inriktning är att samhällsviktig verksamhet själv ska vidta åtgärder för att säkerställa tillräcklig robusthet</i>	30
7.1.3	<i>Exempel på åtgärder</i>	30
7.2	Öka redundans och flexibilitet i nätverk	31
7.2.1	<i>Syftet är att göra näten för elektronisk kommunikation mer robusta</i>	31
7.2.2	<i>Inriktningen är att öka redundans och omkopplingsmöjligheter</i>	31
7.2.3	<i>Exempel på åtgärder</i>	32
7.3	Förbättra skyddet mot fysiska, logiska och elektromagnetiska hot	34
7.3.1	<i>Syftet är att minska risken för att kritiska delar av elektronisk kommunikation slås ut</i>	34
7.3.2	<i>Inriktningen är att vidmakthålla och utveckla skyddet mot nya krav</i>	34
7.3.3	<i>Exempel på åtgärder</i>	35
7.4	Öka kunskapen om informationssäkerhet	36
7.4.1	<i>Syftet är att öka kunskapen om informationssäkerhet</i>	37
7.4.2	<i>Inriktning är att varna, informera och ge stöd om IT-säkerhet och incidenter</i>	37
7.4.3	<i>Exempel på åtgärder</i>	37
7.5	Verka för robust elförsörjning för elektronisk kommunikation och fördjupa samverkan mellan el- och telekomområdena	38
7.5.1	<i>Syftet är att skapa robust elförsörjning för elektronisk kommunikation och robust elektronisk kommunikation för elförsörjningen</i>	38
7.5.2	<i>Inriktningen är att skapa gemensamma strukturer för informationsutbyte och för nyttjande av reservkraft så effektivt som möjligt</i>	38
7.5.3	<i>Exempel på åtgärder</i>	39
7.6	Utveckla samverkan	39
7.6.1	<i>Syftet är att förbättra samverkansformer och rutiner</i>	39
7.6.2	<i>Inriktningen är att utveckla en struktur för ömsesidigt informations- och erfarenhetsutbyte</i>	40
7.6.3	<i>Exempel på åtgärder</i>	40
7.7	Fördjupa det internationella samarbetet	41
7.7.1	<i>Syftet är att utveckla det internationella perspektivet i planering och utformning av beredskapen för allvarliga hot och påfrestningar på samhället</i>	41
7.7.2	<i>Inriktningen är att aktivt delta i internationella fora och utveckla bilaterala kontakter med andra nationer</i>	42
7.7.3	<i>Exempel på åtgärder</i>	42
7.8	Förbättra förmågan till krisledning inom elektronisk kommunikation	43
7.8.1	<i>Syftet är att förbättra förmågan till krisledning inom sektorn elektronisk kommunikation</i>	43
7.8.2	<i>Inriktningen är att genomföra övningar och införskaffa reservutrustning</i>	43
7.8.3	<i>Exempel på åtgärder</i>	43
7.9	Öka effekten av robusthetsåtgärder i näten	45
7.9.1	<i>Syftet är att effektivisera de robusthetshöjande åtgärderna och utveckla samverkan med andra delar i samhället</i>	45
7.9.2	<i>Inriktningen är att kontinuerligt utveckla kunskaperna och förståelsen för den komplexa utveckling som sker</i>	45
7.9.3	<i>Exempel på åtgärder</i>	45
8	Grunder för prioritering av insatser	46
	Ordlista	48

Sammanfattning

Regeringen gav i regleringsbrevet 2002 Post- och telestyrelsen (PTS) i uppdrag att för elektronisk kommunikation redovisa en strategi för hur arbetet ska bedrivas när det gäller åtgärder för att minska konsekvenserna av svåra påfrestningar på samhället i fred och för att öka beredskapen inför höjd beredskap och krig.

PTS har tidigare redovisat nämnda regeringsuppdrag i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2003-2005”, PTS-ER-2003:13, 2003-03-31 och i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2006-2008”, PTS-ER-2006:19, 2006-04-24

Föreliggande rapport redovisar PTS strategi för åren 2009-2011 inom ramen för utgiftsområde 6 ”Försvaret och samhällets krisberedskap”.

PTS redovisar mål för robust elektronisk kommunikation vid allvarliga hot och påfrestningar på samhället i fred.

PTS redovisar principer för samverkan om säkerhet mellan företrädare för allmänna intressen och enskilda aktörer inom elektronisk kommunikation. Utgångspunkten för samverkan ska vara de former för elektronisk kommunikation som under normala förhållanden och fri konkurrens växer fram i samhället. Samverkan med enskilda aktörer ska syfta till att öka medvetenheten om de svåra situationernas krav och att finna lämpliga kompletterande åtgärder för att tillgodose robustheten i elektronisk kommunikation 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 elektronisk kommunikation
2. Ökad redundans och flexibilitet i nätverk
3. Förbättrat skydd mot både fysiska, elektromagnetiska och logiska hot
4. Öka kunskapen om informationssäkerhet
5. Robust elförsörjning för elektronisk kommunikation och fördjupad samverkan mellan el- och telekomområdena
6. Utveckla samverkan
7. Fördjupa internationell samverkan
8. Förbättrad förmåga till krishantering inom elektronisk kommunikation
9. Öka effekten av robusthetsåtgärder 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 elektronisk kommunikation tillgodoses och ett uppdrag att vidta åtgärder för att förebygga och motverka sårbarhet inom sitt sektorsområde.

Enligt 11 § förordning (2006:942) om åtgärder för krisberedskap och höjd beredskap ska PTS planera och vidta åtgärder för att skapa förmåga att hantera en kris och för att förebygga sårbarheter och motstå hot och risker.

1.2 **Strategin är en uppdatering och vidareutveckling av tidigare strategier på området**

Den tidigare strategin sträckte sig mellan 2006 – 2008 och benämndes ”Robusta elektroniska kommunikationer Strategi för åren 2006 - 2008” (PTS-ER-2006:19).

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

”PTS ska för telekommunikation 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 ska bedrivas. Strategin ska avse åren 2003 t.o.m. 2005. Som en grund för strategin ska en risk- och sårbarhetsanalys genomföras. Härvid ska 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 ska redovisas till regeringen med en delrapport senast den 1 oktober 2002 och med en slutrapport senast den senast den 1 april 2003.”

PTS har redovisat nämnda regeringsuppdrag i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2003-2005”, PTS-ER-2003:13, 2003-03-31 och i rapporten ”Robusta elektroniska kommunikationer Strategi för åren 2006-2008”, PTS-ER-2006:19, 2006-04-24

Strategin för åren 2009-2011 är en uppdatering och vidareutveckling av tidigare strategier.

1.3 **Utgångspunkter för strategin med tolkning av begreppen i uppdraget**

1.3.1 Strategin omfattar allmänt tillgänglig elektronisk kommunikation

I och med tillkomsten av lagen (2003:389) om elektronisk kommunikation har det tidigare använda begreppet telekommunikation 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 kopparledningar, 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 behoven av robust elektronisk kommunikation

PTS har utformat strategin med utgångspunkt i gällande politiska inriktning och verksamhetsmässiga struktur för samhällets säkerhet och beredskap i stort. Strategin anger hur olika aktörer kan verka för att tillgodose tillförlitlighet, uthållighet och tillgänglighet hos allmänt tillgänglig elektronisk kommunikation vid allvarliga hot och påfrestningar på samhället i fred.

Strategin anger principer för arbetet med att minska sårbarheten och öka robustheten hos allmänt tillgänglig elektronisk kommunikation. Principerna ska tillämpas under åren 2009 – 2011. 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 robust elektronisk kommunikation. 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 7.2 och 7.3) resp. samplanering mellan berörda aktörer avseende beroenden mellan elsystem och elektronisk kommunikation vid omfattande och långa elavbrott (avsnitt 7.5).

1.3.3 Förklaring till allvarliga hot och påfrestningar i fred, höjd beredskap och krig

Med allvarliga hot och 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. 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. terrorism eller annan avancerad brottslighet avsiktligt söker skada och påverka samhället.

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 i sådana fall tänkbara mål för sabotörer inför ett angrepp och för direkta militära insatser under själva angreppet.

1.3.4 Hot, sårbarheter och åtgärder

Hot och sårbarheter för elektronisk kommunikation kan tolkas i vid mening. Strategin har valt att beskriva dessa i tre steg. De utgör;

1. tänkbara hot mot elektronisk kommunikation vid allvarliga hot och påfrestningar på samhället i fred,
2. den tekniska sårbarheten i kommunikationssystemen för dessa hot samt
3. tänkbara konsekvenser för samhället av störningar i allmänt tillgänglig elektronisk kommunikation.

En och samma åtgärd för att höja säkerheten är ofta verkningsfull såväl för att minska konsekvenserna av allvarliga 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- resp. större kriser 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. I utredningsarbetet har ingått ingångsvärden från PTS ständigt pågående risk och sårbarhetsanalysarbetet, samt genomgång av tidigare utredningar och annat bakgrundsmaterial som bedömts ha relevans för frågeställningarna.

Strävan har varit att ta tillvara erfarenheter från inträffade störningar, exempelvis stormen Per i januari 2007, stormen Gudrun januari 2005, terrorattacken i London 2005, bombdådet i Madrid 2004, det stora teleavbrottet i södra Sverige 2003, teleavbrottet i Uppsala den 2 oktober 2002, tunnelbränderna i Kista 2001 och 2002, isstormen i Kanada 1998 samt elavbrottet i Auckland, Nya Zeeland samma år. Strategin har också tagit tillvara erfarenheter utifrån genomförda övningar exempelvis ”Samvete 2005, Telö 2007 samt Telö 2009. Strategin har även beaktat de på senare år inträffade avsiktliga eller oavsiktliga störningar av logiska system, exempelvis attacker mot routingfunktionen för IP-baserad samtrafik, attacker mot domännamnsystemet (DNS) samt överbelastningsattacker.

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 8.

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 elektronisk kommunikation vid allvarliga hot och påfrestningar. Kapitlet ger framför allt dem som ska tillämpa strategin för robust elektronisk kommunikation en bakgrund om hur samhällets beredskap och säkerhet hanteras i stort.

I kapitel 3 görs en övergripande beskrivning av infrastrukturen för elektronisk kommunikation.

I kapitel 4 redovisas kortfattat tidigare satsningar på robusthetsarbete i elektronisk kommunikation. Dessa satsningar relateras sedan till dagens behov.

I kapitel 5 redovisas ett till dagens förhållanden anpassat mål för robust elektronisk kommunikation vid allvarliga hot och påfrestningar på samhället i fred. 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 6 redovisas principer för samverkan om säkerhet mellan företrädare för allmänna intressen och enskilda aktörer inom elektronisk kommunikation.

I kapitel 7 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 8 redovisas allmänna grunder för prioritering av insatser.

2 Politiska och organisatoriska utgångspunkter för robust 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 (2006:942) om krisberedskap och höjd beredskap” och Krisberedskapsmyndighetens planeringsinriktning ”Samhällets krisberedskap Inriktning för verksamheten till och med 2009”, 0272/2007. PTS har också noterat de successiva förändringarna som indikeras genom Försvarsberedningens rapport ”Säkerhet i samverkan”, (Ds 2007:46). Inriktningar spårbara i propositionen ”Samverkan vid kris – för ett säkrare samhälle” (prop. 2005/06:133), betänkandet ”Alltid redo! En ny myndighet mot olyckor och kriser” (SOU 2007:31) och ”Stärkt krisberedskap – för säkerhets skull”, (prop. 2007/08:92) har också inarbetats i strategin.

2.1 Viktigt att minska sårbarheten i samhällets tekniska infrastruktur

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, elektronisk kommunikation och därmed de ekonomiska systemen 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 fredstida verksamheten, vilken kompletteras med åtgärder inom ramen för säkerhets- och försvarspolitiken.

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.

Statens inflytande över sektorn elektronisk kommunikation har förändrats sedan 1993. Statens inflytande kan idag brytas ner i flera delar;

- Staten kan genom lagstiftning och reglering påverka marknaden. *Här finns dock begränsningar i och med att Lagen om elektronisk kommunikation skall vara harmoniserande med alla medlemsländer inom Europeiska unionen.*
- Staten kan i sin egenskap av stor konsument ställa krav på tjänster och utrustningar i samband med upphandling. *Erfarenheterna visar att det kan vara svårt att få till en samordning inom den offentliga förvaltningen så att den ger effekt. I slutändan är det respektive myndighet och kommun som måste ta hänsyn till den egna budgeten i förhållandet till det egna behovet.*
- Staten kan komplettera den grundläggande förmågan hos operatörerna med åtgärder för att hantera hela hotskalan från allvarliga fredstida kriser till höjd beredskap och krig. Staten kan genom upphandling upphandla robustethöjande åtgärder. Att upphandla robustethöjande åtgärder har visat sig vara en effektiv metod för att bibehålla robustheten i en marknad som präglas av hård prispress och snabb teknikutveckling. Därigenom skapas en förmåga att möta allvarliga hot och påfrestningar samt en handlingsfrihet att kunna anpassa förmågan på medellång och lång sikt. *Det ställer krav på att statsmakterna avdelar medel och har en strategi för sådana åtgärder. Utan medel försvinner denna möjlighet att påverka robustheten i näten för elektronisk kommunikation.*
- Staten kan verka för att skapa former för samverkan och kan vid behov ta på sig rollen att vara samordnande. *Erfarenheter från genomfört arbete under åren 2002 – 2008 visar på flera områden där staten sannolikt måste ta på sig en större samordnande roll. Sektorn består av ca 450 operatörer som var och en i huvudsak tar ansvar för det egna bolaget. Att bedöma dem som en bransch med aktörer som ska ta ansvar utifrån ett samhällsperspektiv för verksamhet utanför det egna bolaget torde inte vara realistiskt.*

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 aktör i sammanhanget är landstingen. Områdesansvaret har stor betydelse eftersom hantering av allvarliga påfrestningar i både fred och krig normalt kräver samverkan mellan flera sektorer och nivåer och som i sin yttersta konsekvens påverkar den lokala nivån.

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 ska ha motsvarande ansvar under kris- och krigssituationer. Likhetsprincipen innebär att en verksamhets organisation och lokalisering så långt som möjligt ska överensstämja i fred, kris och krig. Närhetsprincipen innebär i sin tur att en kris ska hanteras så nära den aktuella krisen som möjligt.

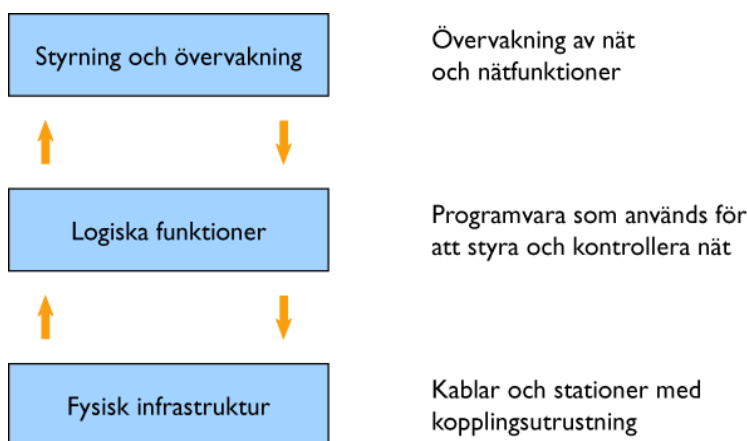
Sektorn elektronisk kommunikation består av flera aktörer med varierande förutsättningar som verkar var och en för sig, vilket gör att sektorn inte alltid kan betraktas som ett gemensamt verksamhetsområde.

3 Infrastrukturen för elektronisk kommunikation och hot, sårbarheter samt beroenden

3.1 Modell av elektroniska kommunikationsnät

I nedanstående modell ges en övergripande modell av elektroniska kommunikationsnät som utgår från tre nivåer. På den första nivån återfinns den fysiska infrastrukturen, exempelvis kopparledningar. Den andra nivån samlar de logiska funktioner som används för att kontrollera och styra de underliggande tekniska systemen där kommunikation bärs fram. Denna nivå utgörs numera av programvara. Den tredje nivån utgörs av funktioner för övervakning och styrning.

Figur 1 Övergripande modell av elektroniska kommunikationsnät



Kommunikationsnätens sammantagna säkerhet och robusthet påverkas av faktorer som kopplas till samtliga nivåer i modellen. En faktor är det sätt varmed operatörer dimensionerat sina tekniska system och i sin planering arbetat för att skapa robusthet. En annan är det sätt som operatörerna övervakar sina nät för att minimera verkan av skador, reducerad kapacitet, överbelastningar eller fel. Dagens moderna kommunikationsnät innehåller en stor mängd logiska funktioner som på olika sätt påverkar robustheten i samspel med den underliggande fysiska infrastrukturen.

3.2 "Internetteknik" används i allt större utsträckning

Den TCP/IP-baserade tekniken baseras, undantaget vissa accessformer, så gott som helt och hållet på standarder framtagna av Internet Engineering Task Force (IETF) beskrivna i s.k. Requests for Comments (RFC). Dessa standarder används i allt större utsträckning för att realisera kommunikation som tidigare

var kretskopplad. När IETF under sjuttio- och åttiotalen konstruerade de olika protokoll (regelverk för kommunikation) som används för Internet, togs liten hänsyn till säkerhets- och kvalitets- (QoS) aspekterna till skillnad från den kretskopplade tekniken, som används i PSTN- och mobiltelefoninäten. Därefter har det på olika sätt försökts att tillföra säkerhet och QoS med diverse tillägg och utökningar av standarder.

3.3 **Ökad sårbarhet till följd av centralisering och konvergerande teknik**

3.3.1 **Ökad centralisering och fjärrstyrning av trafiken ökar beroendet av fungerande förbindelser**

Den tekniska utvecklingen inom området elektronisk kommunikation sker snabbt vilket bl.a. medför ett utökat utbud av tjänster och därmed ett ökande beroende av elektronisk kommunikation. 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 också kan vara placerade utanför rikets gränser.

3.3.2 **Konvergens och komplexa system kan öka sårbarheterna**

Robusthetsproblemen till följd av konvergerande teknik för trafikutbyte kan förväntas att öka. Idag hanteras kretskopplad samtrafik mellan operatörer i separata system. När det gäller paketförmedlad trafik i Next Generation Networks (NGN) och nät med IP Multimedia Subsystem (IMS), kommer all slags trafik som skickas mellan operatörer att hanteras i en och samma typ av utrustning s.k. gränsroutrar med ett kommunikationsprotokoll (Border Gateway Protocol, BGP). BGP som har grundläggande inneboende svagheter.

Efter hand som elektronisk kommunikation konvergerar till IP-baserad teknik, minskar möjligheten till alternativa kommunikationsformer. Samtidigt kan attacker mot den gemensamma tekniken få omfattande konsekvenser om det inte från början vidtas robusthetshöjande åtgärder och byggs in omfattande redundans i systemen och näten för elektronisk kommunikation.

En annan risk är stabiliteten i IMS-komplexet då en rad nya system införs som varit i operativ drift i liten omfattning, och som nu behöver konfigureras, underhållas och övervakas. De flesta operatörer med egen infrastruktur har eller kommer sannolikt att anskaffa IMS.

3.3.3 **Ny GSM-standard bidrar ytterligare till konvergens mot IP**

En funktion som kommer att implementeras inom de närmaste åren är ipx som står för IP Packet eXchange och har utvecklats av GSM Association

(GSMA). Ipx är en standardiserad tjänst baserad på det vanliga IP-protokollet, men med den skillnaden att kvalitén garanteras hela vägen mellan mottagare och sändare. Vanliga Internettjänster, såsom e-post, direktmeddelanden och liknande kommer också att fungera i denna nya miljö, förutom tjänster som normalt hör till mobilen såsom sms och mms. Störst nytta gör sannolikt ipx för de mest krävande realtidstjänsterna, som telefoni och tv-tjänster. Tanken är att IP-telefoni ska kunna användas i mobiltelefonen för att prata med en annan mobiltelefon över långa internationella distanser med högsta talkvalitet. Bilder och meddelanden ska kunna skickas snabbt över hela världen med garanterad största fördröjning för all trafik. Operatörerna får för första gången möjlighet att erbjuda IP-baserade tjänster med garanterad kvalitet.

3.4 Beroendet av externt kontrollerade resurser

3.4.1 Immateriella resurser för trafik baserad på Internetteknik

Internet och andra IP-baserade nät är i många fall beroende av ett antal kritiska immateriella resurser. När det gäller de juridiska och politiska aspekterna för förvaltningen av dessa resurser, är de främsta aktörerna USA:s regering genom DoC (US Department of Commerce), IANA (Internet Assigned Numbers Authority) tillsammans med den privata stiftelsen Internet Corporation for Assigned Names and Numbers (ICANN) och dess rådgivande kommitté Governmental Advisory Committee (GAC). I den globala debatten är EU, Internet Governance Forum (IGF) och Internationella Teleunionen (ITU) viktiga parter.

I den tekniska förvaltningen av Internets resurser har tre typer av aktörer en avgörande roll, operatörerna för rotnamnsservrarna i DNS, registreringsenheterna för toppdomäner t.ex. Stiftelsen för Internetinfrastruktur (IIS) för den svenska toppdomänen .se och de regionala registreringsenheterna för Internets adresser och nummer de s.k. Regional Internet Registries (RIR).

De viktigaste gemensamma resurserna, som förvaltas av ICANN för ett fungerande Internet och av ovan sagda även för att NGN ska fungera, är följande:

- Namnen för de nationella (t.ex. .se) och de generiska toppdomänerna (t.ex. .com) i det globala domännamnssystemet
- Informationsinnehållet i DNS rot (s.k. rotzonen) som bland annat utgörs av adressinformation angående toppdomänerna (ca.260 st).

- IP-adresser av versionerna 4 (IPv4) och 6 (IPv6) för vägval i Internets routrar
- AS-nummer (nummer för autonoma system) som tilldelas operatörer för utbyte av trafik operatörer sinsemellan
- Protokollparametrar som används på Internet

3.4.2 Beroendet av intern och extern DNS-tjänst

IMS använder Session Initiation Protocol (SIP) för att koppla upp IP-förbindelser, till skillnad från de kretskopplade systemen PSTN, GSM och UMTS som använder SS7 (Signalling System 7). SIP använder SIP-adresser som utgör en referens till en IP-adress. För slå upp den IP-adress som motsvaras av en viss SIP-adress används standarden Domain Name System (DNS) som omtalats ovan. Genom att DNS krävs i IMS, har ett nytt beroende uppstått som tidigare endast fanns i Internetsammanhang. DNS är idag mycket robust och motståndskraftigt mot störningar beroende på att det är så distribuerat och har tillgång till en avsevärd sammanlagd kapacitet. De IMS-system som vanligen kommer att ingå i NGN kommer att bli beroende av såväl interna DNS-system som det globala DNS, vilket innebär att de svagheter som finns i DNS-protokollet ärvs in. Stora operatörer kommer förmodligen ha abonnenter som försöker angripa DNS - även operatörens interna DNS-systemen. ICANN/IANA (Internet Corporation for Assigned Names and Numbers/Internet Assigned Numbers Authority) har ansvar för *innehållet* i rotzonen som innehåller alla referensinformation till alla toppdomäner för det globala Internet och att införa ändringar som fås från toppdomän-administratörerna och som rör toppdomänernas namnservrar. Ytterst är det alltså (maj 2009) USA:s handelsdepartement som godkänner förändringar och som sen operativt utförs av den driftsansvariga organisationen, säkerhetsföretaget Verisign. Detta sker i enlighet med ett avtal s.k. Joint Project Agreement (JPA) som dock löper ut den 30 september 2009. Vad som händer därefter är oklart när denna strategi skrivs. För *distributionen* av rotzonens adressinformation ligger emellertid ansvaret inte hos ICANN utan på ett antal olika organisationer, som hanterar driften av rotservrarna och ser till att de kan svara på frågor som ställs till dem. Ansvaret för driften är inte formaliserat genom skriftliga avtal med ICANN. Även om det inte är troligt, kan de som hanterar driften i princip upphöra med sin verksamhet när som helst utan att något ansvar kan utkrävas.

3.5 **Ny version av Internet Protocol (IP) kommer att införas vid sidan av det nuvarande**

Dagens Internet-kommunikation bygger på protokollet IPv4 (Internet Protocol version 4) som kommer att fortsätta dominera under flera år framöver. Nästa version kallas IPv6 och av flera skäl är det hög tid att det börjar införas. Det är inte frågan om en omedelbar eller heltäckande övergång till IPv6 där det nya protokollet ersätter det gamla, utan snarare att ytterligare ett protokoll införs vid sidan om det befintliga.

De tillgängliga adresserna via IPv4 kommer att ta slut – på vissa håll kanske redan under 2011. Det är bristen på adresser som förväntas bli den starkaste drivkraften för nätoperatörer och tjänsteleverantörer att satsa på IPv6, som erbjuder ett adressutrymme för att täcka Internets behov för överskådlig framtid. Om aktörerna väntar för länge med att påbörja införandet av IPv6 kan det uppstå situationer där berörda aktörer tvingas ta till skyndsamma åtgärder med risk för mindre bra lösningar som kan hota stabiliteten.

Standarden IPsec är inbyggd i IPv6 till skillnad mot IPv4 där det går att installera som tillägg. IPsec ger möjlighet till signering och/eller kryptering av meddelanden för ökad tillit till äkthet och informationsintegritet.

En annan fördel för slutanvändaren är bättre åtkomst till Internet beroende på att varje terminal kan få en egen globalt unik adress. I dag används i stor utsträckning en metod för att spara adresser som går ut på att översätta den globalt unika adressen till en adress som bara fungerar lokalt bakom brandvägg inom användarens lokala nät s.k. Network Address Translation (NAT). Många av framtidens 3G-tjänster, som exempelvis push-tjänster och snabbmeddelanden, får genom att kunna använda globalt unika adresser en optimal teknisk lösning där tillgängligheten förbättras mellan de kommunicerande parterna (end-to-end) när man slipper den på olika sätt hämmande adressöversättningen. IPv6 möjliggör därmed effektivare användning av tjänster såsom bredbandig Internetuppkoppling för hushåll, peer-to-peer och den starkt växande marknaden för maskin-till-maskin-tjänster.

Mobil kommunikation kommer från och med nu och framöver att behöva fler IP-adresser vilket möjliggörs tack vare IPv6. Detta är också orsaken till att IPv6 är standard i nuvarande och kommande releaser av 3G/UMTS som tas fram av 3GPP.

Leverantörer av mjukvara för Internets domännamnssystem (DNS) har sen flera år infört stöd för att hantera IPv6-adresser.

4 Arbetet med robust elektronisk kommunikation görs utifrån samhällets behov

4.1 Tidigare satsningar på robusthet i elektronisk kommunikation inriktades främst mot totalförsvarets behov

Sedan länge har det varit av betydelse att inom det svenska totalförsvaret ha tillgång till fungerande elektronisk kommunikation i händelse av höjd beredskap och krig. Omfattande insatser har därför successivt genomförts för att minska systemens sårbarhet och skapa förutsättningar för fungerande elektronisk kommunikation 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 elektronisk kommunikation. 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 elektronisk kommunikation. De ständiga förändringarna gör sammantaget att det finns behov av en strategi som är anpassad för att löpande kunna tillgodose robustheten i elektronisk kommunikation.

4.2 Åtgärder krävs för att säkerställa tillförlitligheten till elektronisk kommunikation

Samhällets beroende av elektronisk kommunikation inklusive Internet gör att det ställs höga krav på tillförlitligheten avseende elektronisk kommunikation. Ett stort antal åtgärder måste genomföras för att tillräckligt hög tillförlitlighet ska kunna uppnås i förbindelser, knutpunkter och annan utrustning. Risken för olyckor och misstag måste reduceras och konsekvenserna minimeras om de ändå inträffar. Steg måste tas för att förhindra obehörig avlyssning eller

förändring av information under överföring. Utrustning för viktiga samhällstjänster på Internet bör fysiskt skyddas mot störningar och avbrott.

Antalet svaga punkter måste minimeras, genom analys och åtgärder vid utbyggnad och utveckling. Eftersom möjligheterna att skydda nätets alla delar mot olyckor och fysiska angrepp är begränsade bör det, i så stor utsträckning som möjligt, finnas redundans för utrustning och förbindelser.

Den logiska infrastrukturen består bl.a. av ett stort antal protokoll och program. Många sårbarheter har identifierats i dessa och fler kommer troligtvis att upptäckas framöver. För att öka robustheten i den logiska infrastrukturen för elektronisk kommunikation måste protokoll och program som är mest kritiska för nätets funktion identifieras, uppmärksammas och eventuellt åtgärdas.

Andra åtgärder är att genom olika utbildnings- och informationsinsatser öka kompetensen hos såväl konsumenter som tjänstetillhandahållare för att de ska kunna ställa adekvata krav på tillgänglighet, kapacitet och kvalitet vid beställning/upphandling av olika tjänster. Behoven hos privat och offentlig sektor samt enskilda användare kan tillfredsställas genom tydliga kravställningar och enhetliga SLA (Service Level Agreement).

För att uppnå hög tillgänglighet är det viktigt att tillse nätets robusthet. En stor del av ansvaret för robustheten i nätinfrastrukturen ligger hos operatörerna som inom ramen för vad som är kommersiellt möjligt på en konkurrensutsatt marknad, vidtar vissa åtgärder för att skydda sina respektive delar av infrastrukturen mot störande eller förstörande incidenter. Konkurrensen kan vara en drivkraft för att operatörerna ska upprätthålla god beredskap och åtgärda störningar och fel som uppstår samtidigt som konkurrensen kan leda till besparingar som gör att förebyggande åtgärder för att öka robustheten minimeras. En modell för att förbättra nätets robusthet är samverkan.

Samverkan mellan kommersiella aktörer kan vara känsligt av flera skäl, bl a konkurrens mellan aktörerna. För att inte samverkan ska riskera att uppfattas som kartellbildning krävs att staten tar sin roll och del i detta arbete.

4.3 **Fortsatta åtgärder för ökad robusthet och krishanteringsförmåga i såväl krig som fred**

Åtgärder har vidtagits för att minska sårbarheten och öka robustheten i elektroniska kommunikationsnät exempelvis genom förstärkning av reservkraft och ökad redundans. Redundans kan beskrivas som fler förbindelser som

skapar flera maskor i näten vilket ger möjligheter att koppla förbi skadade delar av näten.

Under de senaste åren har arbetet främst koncentrerats till att förstärka reservkraftsförsörjningen, förbättra redundansen och att utveckla krishanteringsförmågan genom olika samverkansformer och övningar.

4.3.1 Samverkan i krishantering genom den Nationella Telesamverkansgruppen (NTSG)

Krisledningsförmågan hos sektorns aktörer har förbättrats genom satsningar på olika former av utbildningar i krishantering och kontinuitetsplanering samt övningar. Inom sektorn har en Nationell Telesamverkansgrupp (NTSG) bildats, vars syfte är att i samverkan stödja uppbyggnaden av infrastrukturen för elektronisk kommunikation i händelse av omfattande avbrott.

I Sverige har hanteringen av information om driftstörningar i näten för elektronisk kommunikation utvecklats i samverkan mellan stat och näringsliv benämnt Gemensam lägesuppfattning (GLU). De teleoperatörer som är medlemmar i NTSG deltar tillsammans med PTS i ett ”Private Public Partnership (PPP)” med syfte att reducera störningar inom sektorn, minska dess effekt för andra samhällssektorer som är beroende av elektronisk kommunikation, samt öka samhällets förmåga att hantera konsekvenser av störningar inom elektronisk kommunikation.

4.3.2 GLU - ett system för gemensam lägesuppfattning av störningar och avbrott

GLU är en kombination av metod, gemensamma normer och teknik. Metod är en viktig beståndsdel i GLU. Att få konkurrenter och olika aktörer att samverka för att få fram en gemensam syn/lägesbild är ett grundläggande arbete.

Genom GLU kan respektive teleoperatör presentera detaljerad information om status och prognos för pågående störningar som påverkar kundernas möjlighet att kommunicera. Informationen finns allmänt tillgänglig via Internet. Informationen kommer även att finnas tillgänglig med hög robusthet för att stödja behoven av information hos aktörer som upprätthåller funktioner som är viktiga för samhället vid en kris exempelvis områdesansvariga myndigheter, Försvarsmakten, elförsörjning, betalningsväsendet m fl.

Teleoperatörerna rapporterar till SOS Alarm om störningar som påverkar möjligheten att använda nödnumret 112. Informationshanteringen i GLU ger teleoperatörerna möjligheter att informera SOS Alarm på ett gemensamt och strukturerat sätt. Ett syfte med att arbeta med samma format är att det

underlättar SOS Alarms analysarbete hur pågående störningar påverkar möjligheterna att nå nödnumret 112 och övrig krishantering i samhället.

I GLU har deltagarna gemensamt utarbetat en ”branschöverenskommelse” och skapat en ensad eller likartad information vad gäller innehåll, hantering och presentation.

GLU har finansierats av PTS, Hi3G, Access AB (3), Telenor Sverige AB, Telia Sonera AB, TDC Song, Tele2 Sverige AB, Stadsnätsföreningen samt EU-kommissionen (inom ramen för European Programme for Critical Infrastructure Protection),

En viktig målsättning är att det som genomförs i GLU ska kunna genomföras internationellt, t ex ska GLU kunna införas i andra stater i EU. Det finns ett internationellt intresse för GLU. Genom att bidra till att skapa robust elektronisk kommunikation i Europa skapas robusthet för användarna av elektronisk kommunikation i Sverige.

4.3.3 Alternativ överföring av korrekt spårbar tid

PTS har under ett antal år bedrivit forskningsprojekt tillsammans med Sveriges Tekniska Forskningsinstitut (SP) rörande överföring av inhemsk producerad korrekt spårbar tid över optiska fibernät. Syftet med projektet är att göra Sverige mindre beroende av utländska radioburna tidskällor. Detta gäller främst GPS, som Sverige inte har kontroll över samtidigt som dessa signaler kan manipuleras eller störas så att centrala funktioner i elektroniska kommunikationssystem störs eller upphör att fungera.

4.3.4 Stärkt robusthet för funktionen för IP-samtrafik

Det som möjliggör att Internet är ett globalt nätverk, är att trafik kan flyta mellan olika operatörers nät. Ett stort trafikutbyte mellan olika operatörer, kan innebära att Internettrafik eller annan IP-baserad kommunikation genom illvilligt agerande eller misstag styrs fel. Resultatet kan bli att användare inte når fram till sökt webbplats eller att e-post inte kommer fram.

Det finns svagheter och sårbarheter i funktionen för trafikutbyte som kan utnyttjas för attacker. Även om protokollen i sig inte attackerats, kan tillgänglighetsattacker orsaka svåra följder t.ex. genom att routerns processorkapacitet, minne eller förbindelser överbelastas, så att funktionen helt eller delvis slås ut. Under 2007 genomförde PTS ett projekt som testade sårbarheter i IP-samtrafikfunktion med analys av vilka konsekvenserna blir för slutanvändare. Testet påvisade att funktionen under vissa omständigheter är sårbar. I slutrapporten (PTS-ER-2007:14) ingår en uppdaterad Best Current

Practice (BCP) för aktörer som operativt ansvarar för en knutpunktsfunktion för samtrafik (utbyte) av IP-/Internettrafik. Allmänt tillgängliga knutpunkter för utbyte av Internettrafik s.k. Internet Exchange Points (IXP) kommer i framtiden att få allt större betydelse i framtiden för utbyte av all slags IP-baserad trafik mellan operatörer. Det föreligger ett tydligt behov att stärka robustheten i den logiska funktionen som hanterar trafikutbytet.

4.3.5 Behov av ökad tillgänglighet och tillförlitlighet till DNS

Domännamssystemet är sårbart genom att namnservrarnas förbindelse till Internet kan attackeras eller att angrepp sker mot namnservrarna i sig. Tillgängligheten kan hotas vid överbelastning.

När det gäller tillförlitligheten till DNS, går det att förfalska adressinformationen som förmedlas. Det kan leda till att användare hamnar på fel webbplats eller att e-post skickas till fel destination. För att få trovärdighet till mottagna svar, måste en frågeställare till Internets Domännamssystem (DNS) kunna verifiera varifrån informationen kommer och att informationen inte förändrats på vägen. Det kan göras genom att använda DNSSEC (DNS Security Extensions), som är en standard baserad på kryptografiska metoder för att säkerställa namnsuppslagningar i DNS. Användare som söker en tjänst på en webbplats kan därmed vara säkra på att de befinner sig på den riktiga webbplatsen och inte på en falsk kopia.

PTS har arbetat med DNSSEC sen 2005 då en test genomfördes av införande av DNSSEC dokumenterat i en rapport (PTS-ER-2006:36). Vidare har PTS främjat införande av tekniken genom att som den första statliga myndigheten i världen införa DNSSEC för sin egen s.k. zon, pts.se, vilket skedde i september 2008.

5 Målen för robust elektronisk kommunikation

Målet är att elektronisk kommunikation ska vara uppbyggd på ett sådant sätt

- att kriser i fred inte leder till oacceptabla avbrott eller störningar
- att konsekvenser av allvarliga hot och påfrestningar på samhället i fred minimeras och
- att förmågan kan anpassas till de krav som ställs i ett förändrat säkerhetspolitiskt läge

Inriktningen för att nå målet/målen är att vidmakthålla och öka robustheten i elektronisk kommunikation.

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 ska 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 de olika operatörernas 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 elektronisk kommunikation är

Slumpmässiga händelser och situationer

- Tekniska fel på utrustningar
- Felaktig hantering av utrustning

- Olyckor såsom brand, CBRN¹ och dylikt
- Fysisk åverkan eller skada
- Stora störningar i elsektorn
- Extrema vädersituationer och andra naturkatastrofer
- Skador på logiska funktioner
- Överbelastning av fysisk och logisk kapacitet
- Influensapandemi

Avsiktliga händelser och situationer

- Terroristattacker
- Fysisk åverkan eller skada
- IT-relaterade attacker, exempelvis virus, maskar, trojaner
- Icke konventionella attacker, CBRN
- Attacker riktade mot kritiska logiska funktioner, exempelvis gränsrouting och DNS
- Överbelastningsattacker av fysisk och logisk kapacitet

5.1 **Elektronisk kommunikation ska ha sådan kapacitet att viktiga samhällsfunktioner kan upprätthållas även vid kriser**

Vid påfrestningar på samhället i fred ska elektronisk kommunikation ha sådan kapacitet att de uthålligt kan medverka till att viktiga samhällsfunktioner kan upprätthållas. Sådana funktioner är bl.a. ledning, polisiär verksamhet, 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.

¹ Chemical, biological, radiological, nuclear

För att uppnå målet ställs krav på att även slutanvändare tar ansvar för sin del i den kedja av elektronisk kommunikation som måste fungera vid elektroniskt utbyte av information.

5.2 **Elektronisk kommunikation ska medverka till att säkerställa livsnödvändiga funktioner och möjliggöra ett effektivt försvar**

Tänkbara hot vid höjd beredskap och krig är främst sabotage eller begränsade angrepp med militära medel mot elektronisk kommunikation. Möjligheter ska finnas att på sikt anpassa elektronisk kommunikation så att de kan motstå dessa hot.

Vid hotande väpnat angrepp eller i krig ska elektronisk kommunikation kunna medverka till att säkerställa livsnödvändiga funktioner och till att möjliggöra ett effektivt försvar.

Sverige ska sträva efter att kunna ställa civil kompetens och civila resurser inom sektorn elektronisk kommunikation till förfogande för internationell krishantering.

6 Samverkan

Att öka robustheten och tillförlitligheten till elektronisk kommunikation i händelse av en kris kräver omfattande förebyggande och reaktiv samverkan mellan operatörerna och myndigheten inom sektorn elektronisk kommunikation. Därutöver krävs att sektorns aktörer samverkar med näringslivsaktörer inom andra sektorer, centrala och regionala myndigheter samt kommuner.

Samverkan ska utgå från de former för elektronisk kommunikation som under normala förhållanden och i fri konkurrens växer fram i samhället. Arbetet ska utveckla rutiner för effektiv samverkan och öka förståelsen för olika aktörers verksamheter och ansvarsområden.

Inom sektorn elektronisk kommunikation kan staten genom privatoffentlig samverkan med enskilda aktörer med exempelvis utnyttjande av ekonomiska incitament och överenskommelser öka robustheten i elektronisk kommunikation. Informationsutbyte, gemensamma krisövningar, kompatibla system, formaliserade kontaktnät, informella kontaktnät och praktiska försök utgör viktiga medel för koordinering och samverkan.

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

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

7 Åtgärdsområden

PTS anser det angeläget att insatser genomförs i nedan presenterade områden för att vidmakthålla och öka robustheten i elektronisk kommunikation.

Valet av områden grundar sig på en bedömning av flera faktorer bl.a. de hot mot elektronisk kommunikation som finns i dagens säkerhetspolitiska läge, systemens utformning och samhällets ökade beroende av elektronisk kommunikation. Valet av områden utgår också utifrån att utveckla samhällets krisberedskap. Samhällets krisberedskap som behövs för att hantera allvarliga kriser i samhället utgörs av tre delar; krisledningsförmågan, den operativa förmågan samt förmågan i samhällsviktig verksamhet att motstå allvarliga störningar.

Vissa åtgärder inom ett antal av dessa områden är inte så kostnadskrävande, men kan vara personellt resurskrävande. Exempel på sådana åtgärder är utbyte och spridning av information, samverkan, samarbete, internationell samverkan och övningar. De bedöms ge hög effekt om än med begränsad varaktighet, varför upprepade insatser därför är nödvändiga.

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

7.1 **Stimulera till ett ökat användaransvar inom elektronisk kommunikation**

Samhällsviktiga verksamheter ska uppmärksammas på att ta ansvar för sin del i den kedja av elektronisk kommunikation som måste fungera vid elektroniskt utbyte av information.

7.1.1 Syftet är att stimulera samhällsviktiga verksamheter att skapa en god robusthet för sin elektroniska kommunikation

Utifrån den egna verksamheten varierar användarnas krav på säkerhet i elektronisk kommunikation. Vissa verksamheter klarar utan större olägenheter relativt långa avbrott och kvalitetssänkningar i de tjänster som erbjuds, medan andra har små eller inga toleranser mot avbrott eller kvalitetsförsämringar.

Skydd mot alla tänkbara hot kan aldrig garanteras. Organisationer som bedriver samhällsviktig verksamhet, kommer alltid att ha högre krav på säkerhet än vad som normalt erbjuds. Det är inte en realistisk ambition att överallt anpassa

robustheten i elektronisk kommunikation efter organisationer med de högsta kraven på säkerhet. Det är därför viktigt att ansvariga för elektronisk kommunikation inom samhällsviktig verksamhet har en bild av de egna behoven och tydligt kan ställa krav exempelvis på daglig drift vid upphandling. Åtgärder måste vidtas för att minska risker som föreligger. Det kan göras genom att i avtal med operatörer ställa krav på tillgänglighet, anskaffa reservalternativ, sätta upp lokalt skydd mot såväl dataintrång som fysiskt intrång etc.

Detta åtgärdsområde syftar till att stimulera samhällsviktig verksamhet att utifrån egna behov skapa robusthet i sin elektroniska kommunikation. Därmed förbättras de grundläggande förutsättningarna för att samhällsviktig verksamhet ska ha tillgång till uthållig och tillförlitlig elektronisk kommunikation också i samband med påfrestningar på samhället i fred, höjd beredskap och krig.

7.1.2 Inriktning är att samhällsviktig verksamhet själv ska vidta åtgärder för att säkerställa tillräcklig robusthet

I första hand ska åtgärderna inriktas på att samhällsviktig verksamhet själv ska vidta åtgärder för att tillgodose den egna tillgången till robust elektronisk kommunikation. PTS kan i detta sammanhang bidra till att informera om olika åtgärder som organisationer kan vidta för att öka robustheten.

7.1.3 Exempel på åtgärder

Tillhandahålla information och rådgivning

För vissa verksamheter kan det vara alltför kostsamt att hålla egen kunskap om hur man ska säkerställa sin elektroniska kommunikation. PTS kan tillhandahålla information och rådgivning i frågor som rör elektronisk kommunikation 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 samhällsviktig verksamhet i frågor som rör elektronisk kommunikation.

Medverka i uppföljningsstudier

Erfarenheter, som visar vilka konsekvenserna kan bli vid större störningar, bör spridas till andra intressenter, exempelvis områdesansvariga myndigheter. Erfarenheterna är även användbara för PTS som underlag för prioritering av åtgärder. Det är därför viktigt att ta initiativ till och medverka i uppföljningsstudier som genomförs och utreda vilka konsekvenserna varit vid större störningar. (Jämför med motsvarande åtgärd under åtgärdsområdet 7.9 Öka effekten av robusthetsåtgärder i näten.)

7.2 Öka redundans och flexibilitet i nätverk

Elektronisk kommunikations känslighet för störningar ska minskas.

Kompletterande åtgärder ska göras för att öka redundansen i näten utöver vad som är kommersiellt motiverat så att samhällsviktiga behov av elektronisk kommunikation kan tillgodoses vid allvarliga hot och påfrestningar på samhället i fred. Möjligheter ska tas tillvara att vidta sådana åtgärder i samband med utbyggnad 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 hopkoppling mellan olika operatörers nät skulle kunna skapa.

Studier för att följa utvecklingen avseende möjligheterna att prioritera trafik i elektronisk kommunikation ska genomföras.

Försvarmaktens behov av tillgång till de allmänt tillgängliga näten ska uppmärksammas.

7.2.1 Syftet är att göra näten för elektronisk kommunikation mer robusta

Detta åtgärdsområde syftar i huvudsak till att göra näten för elektronisk kommunikation mer robusta genom att minska risken för avbrott. En konsekvens av att nätfunktioner och tjänster fortlöpande centraliseras och att näten i allt större utsträckning fjärrövervakas och fjärrstyrs, är att delar av landet kan bli avskurna vid skador i näten. Förbindelseavbrott med centrala delar i näten kan innebära att även lokal kommunikation inte kan upprätthållas. Risken är särskilt stor för norra Sverige, Gotland och delar av landet med begränsat befolkningsunderlag. Risken för samtidigt förekommande störningar på flera ställen är särskilt stor vid kriser i samhället.

7.2.2 Inriktningen är att öka redundans och omkopplingsmöjligheter

Åtgärderna inom detta område ska 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 medge.

Åtgärderna inom detta område bör beakta att i en krissituation är de samhällsviktiga aktörerna ofta beroende av fungerande elektronisk kommunikation 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 ska 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.

Vid satsningar på åtgärder för att förbättra redundans och flexibilitet i näten för elektronisk kommunikation ska följande fyra förhållanden beaktas:

- **Platser med stor sannolikhet att drabbas av störningar.** Det är rimligt att satsningar görs där störningar vid allvariga hot och påfrestningar på samhället 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 verksamheter 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.

7.2.3 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.

Utveckla möjligheter till prioritering

I en kris kan det vara många användare som samtidigt vill utnyttja elektronisk kommunikation, 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.

Tillföra extra noder och hopkopplingspunkter

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.

Genom att tillföra hopkopplingspunkter och länkar mellan olika nätägares nät går det där det är tekniskt möjligt att skapa ökad redundans.

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 fysiskt åtskilda framföringsvägar.

Investeringar i extra noder eller redundanta förbindelser kan genomföras efter gemensamma analyser av nätägare och PTS. Den privatoffentliga samverkan måste hållas ständigt aktuell för att PTS och nätägarna ska kunna vidta åtgärder på ett kostnadseffektivt sätt.

Ett mål är att redundanta förbindelser ska kunna ha lika kapacitet o kvalitet (fördröjning, jitter, paketförluster etc.) som ordinarie förbindelse. Tjänster som kräver hög bandbredd (HD-TV, 3-dimensionella bilder etc.), för exempelvis överföring av bilder från skadeplats, instruktion för första hjälpen, bör också kunna fungera i de redundanta alternativen.

Samutnyttja nät vid extraordinära situationer

Det finns idag ett flertal nät för elektronisk kommunikation 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 ska kunna samutnyttja nät om skador i näten uppstår.

Genomföra tester och övningar

För att säkerställa redundans måste det genomföras tekniska tester där möjligheter till omdirigering av trafik utvärderas. Likaså måste samövningar

mellan operatörer genomförs för att säkerställa att samverkan mellan operatörer fungerar i kritiska situationer.

7.3 **Förbättra skyddet mot fysiska, logiska och elektromagnetiska hot**

Noder med kritiska funktioner har placerats i anläggningar som skyddar mot fysisk och elektromagnetisk åverkan. Fortsatta investeringar i dessa anläggningar handlar om att vidmakthålla och anpassa dem efter nya krav. Övriga viktiga noder som inte är förlagda i bergtrum behöver också skyddas mot skador på grund av olyckor och avsiktlig skadegörelse.

7.3.1 Syftet är att minska risken för att kritiska delar av elektronisk kommunikation slås ut

Elektronisk kommunikation utgörs av tekniska system, placerade på platser som ofta är relativt lätt fysiskt åtkomliga och är geografiskt utspridda i landet. Det gör dem sårbara för slumpmässiga hot och åtkomliga för avsiktliga angrepp.

Förbättrat skydd ska hindra eller begränsa effekten av direkta fysiska och logiska hot. Det ska 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.

7.3.2 Inriktningen 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 ska i första hand dra nytta av de resurser som redan har byggts ut. Tillkommande centrala ledningsorgan och viktiga noder i nät med hög överföringskapacitet ska också uppmärksammas. Andra 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 7.2 ska 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 dubblas. Utspridning och många möjligheter till vägval i maskformiga nät kan också ge robust elektronisk kommunikation utöver ett bra skydd för centrala noder.

Internets logiska infrastruktur består bl.a. av ett stort antal protokoll och program. Många sårbarheter har identifierats i dessa och fler kommer troligtvis att upptäckas framöver. En strävan efter ett säkrare Internet bör koncentreras mot att identifiera protokoll och program som är kritiska för Internets funktion såsom protokoll för domännamnsystemet, trafikutbytet mellan operatörer samt införandet av ett nytt IP-protokoll vid sidan av det ännu förhärskande IPv4.

För att öka domännamnsystemets motståndskraft mot överbelastnings-attacker, är det viktigt att namnservrarna för en zon finns i flera kopior på skilda fysiska och logiska nät samt har överkapacitet vad gäller minne och bearbetningsförmåga.

Då protokollet för gränsrouting, BGP; saknar faciliteter för att garantera äkthet och källa, finns även risk för att falsk routinginformation sprids mellan operatörerna. Detta kan leda till att trafiken förmedlas till felaktiga destinationer. Konsekvenserna kan bli svåra i särskilda fall och medföra att delar av Internet eller andra IP-baserade nät blir mer eller mindre otillgängliga.

7.3.3 Exempel på åtgärder

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 skydd mot elektriska och elektromagnetiska hot.

Domännamnsystemet, DNS

Fortsätta informera om vikten av att se till att namnservrarna för en s.k. zon dvs. del av en domän som ingår i ett driftmässigt ansvarsområde, dels finns i flera kopior på skilda fysiska och logiska nät, dels har överkapacitet vad gäller minne och bearbetningsförmåga för att kunna stå emot attacker.

PTS kommer att på olika sätt, bland annat genom att stödja utbildningsverksamhet, fortsätta att befrämja införande av DNSSEC hos främst samhällsviktiga aktörer. Som ett led i det arbetet har PTS infört DNSSEC för sin egen zon pts.se hösten 2008.

Gränsroutning

För att skydda gränsroutningen kan exempelvis följande åtgärder vidtas:

- Infrastrukturskydd genom listor för åtkomstkontroll s.k. Access Control List (ACL), vilket ger skydd för att förhindra utomstående från att kontakta routrar och annan utrustning i infrastrukturen.
- Spoofing-skydd: filtrering för att i möjligaste mån upptäcka och förkasta trafik där avsändaradressen förfalskats.
- Filtrering av BGP: filtrering av otillåtna adresser s.k. bogons dvs. oanvända adressblock och andra felaktiga rutter över peeringförbindelser.
- Filtrering inom det interna nätet
- Tillse att routrarna är optimalt konfigurerade och har tillräcklig kapacitet vad gäller minne och processorkraft så att också onormala nivåer på trafik och routinginformation kan hanteras

IPv6

Enligt IANA (Internet Assigned Numbers Authority) som ansvarar för tilldelningen av IP-adresser, kommer dagens version IPv4 att ta slut någon gång under 2011 eller 2012. Det är därför nödvändigt att innan dess börja införa det nya IPv6-protokollet, vars främsta fördel är det stora adressutrymmet, för fortsatt gynnsam utveckling av nätverk och tjänster. Operatörer, tjänstetillhandahållare och konsumenter måste förr eller senare ta steget över till IPv6, för att i framtiden kunna förmedla, tillhandahålla respektive konsumera tjänster. IPv6-införande är både kostsamt och krångligt och ger dessutom inget omedelbart mervärde. Sannolikt vill ingen börja förrän det blir absolut nödvändigt, och då kan det bli både dyrt samt medföra risk för mindre bra lösningar. Det således lämpligt att börja i tid, varför delar av offentlig sektor bör föregå med gott exempel och göra sina webbplatser åtkomliga såväl via IPv4 som via IPv6. I detta sammanhang är det viktigt att se till att robustheten bibehålls trots att två IP-protokoll hanteras samtidigt.

7.4 Öka kunskapen om informationssäkerhet

PTS ska i sitt arbete med informationssäkerhet och i samverkan med andra berörda aktörer i samhället beakta angrepp mot elektronisk kommunikation och andra allvarliga störningar som kan förekomma i fred, höjd beredskap och krig. Insatserna kan omfatta analyser, tekniska tester och information och investeringar för att försvåra kvalificerade informationsteknologiska angrepp.
--

7.4.1 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 elektroniska kommunikationssystem, men även utnyttja dessa system för att angripa andra samhällsviktiga funktioner.

7.4.2 Inriktning är att varna, informera och ge stöd om IT-säkerhet och incidenter

PTS har ansvaret för Sveriges IT-incidentcentrum (Sitic), en funktion som har rollen av myndighets- och stats-CERT (Computer Emergency Response Team) i Sverige. Det övergripande syftet med en CERT är att mildra eller förhindra negativa effekter för intressenterna vid inträffade IT-incidenter. Sitic gör detta genom att publicera varningsinformation om tekniska sårbarheter i IT-system, och med direkt stöd bistå drabbade myndigheter. I rollen som stats-CERT arbetar Sitic med att distribuera information till nät- och systemägare om förhållanden som direkt eller indirekt påverkar säkerheten negativt; exempel här är botnets, phishing sajter eller sårbara system.

Det samordnande ansvaret för myndigheternas övergripande informationssäkerhetsarbete åvilar Myndigheten för Samhällsskydd och Beredskap (MSB). PTS ska stödja MSB i informationssäkerhetsarbetet i syfte att få fram relevant information till samhällsviktiga användare.

7.4.3 Exempel på åtgärder

Bidra till höjd säkerhetsnivå

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

Genomföra tekniska tester

Tekniska tester för att utvärdera skyddet mot IT-relaterade hot mot elektronisk kommunikation genomförs.

7.5 **Verka för robust elförsörjning för elektronisk kommunikation och fördjupa samverkan mellan el- och telekomområdena**

Elektronisk kommunikation är beroende av fungerande elförsörjning samtidigt som samhället har behov av fungerande elektronisk kommunikation vid störningar i elförsörjningen. Det ömsesidiga beroendet kräver att samverkan fördjupas och utvecklas mellan ansvariga myndigheter och operatörer inom elsektorn och sektorn elektronisk kommunikation. Ytterligare satsningar ska göras för att minska konsekvenserna av det ömsesidiga beroendet vid avbrott.

7.5.1 Syftet är att skapa robust elförsörjning för elektronisk kommunikation och robust elektronisk kommunikation för elförsörjningen

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 elektronisk kommunikation.

Det finns ett ömsesidigt beroende mellan elektronisk kommunikation och elförsörjningen. Vid störningar i elförsörjningen är fungerande elektronisk kommunikation väsentlig för att kunna hantera problem, såväl inom elförsörjningen i sig som inom verksamheter som drabbas av brister i elförsörjningen.

PTS och Svenska Kraftnät (SvK) leder flera samverkansprojekt mellan aktörerna i de bägge sektorerna. Fördjupad samverkan mellan dessa områden är ett viktigt medel för att minska sårbarheten mot störningar inom bägge sektorerna.

7.5.2 Inriktningen är att skapa gemensamma strukturer för informationsutbyte och för nyttjande av reservkraft så effektivt som möjligt

PTS samverkar med Svenska Kraftnät, Statens Energimyndighet och andra aktörer på elmarknaden och marknaden för elektronisk kommunikation för att minska risken för störningar. Strukturer för ömsesidigt informations- och erfarenhetsutbyte bör utvecklas för att förbättra och snabba upp kontakten mellan representanter för elsektorn och sektorn elektronisk kommunikation.

Samarbetet mellan el- och telekomområdena bör leda till samordnade åtgärder för att höja beredskapen inom såväl el som elektronisk kommunikation. Målet

är att kunna utnyttja respektive systems styrkor och minimera dess svagheter. Denna samverkan bör även innefatta planering för krishantering.

Behovet av elektronisk kommunikation 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 robust elförsörjning för elektronisk kommunikation.

7.5.3 Exempel på åtgärder

Investera i robust elförsörjning

Satsningar på lösningar för reservkraft ska ske i samverkan med operatörerna inom sektorn för elektronisk kommunikation och där så är möjligt med representanter för elförsörjningen.

Där gemensamma intressen finns från såväl elsektorn som sektorn elektronisk kommunikation avser PTS att utöka samverkan avseende åtgärder som reducerar konsekvenserna av det ömsesidiga beroendet.

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

Utföra gemensamma tester och övningar

Övningar och tester där representanter från både elsektorn och sektorn elektronisk kommunikation deltar främjar förståelse och samverkan, samt höjer medvetenheten om det ömsesidiga beroendet mellan dessa båda infrastruktursystem.

7.6 Utveckla samverkan

Utvecklade samverkansformer mellan berörda aktörer är en förutsättning för effektiv krishantering.

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

7.6.1 Syftet är att förbättra samverkansformer 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 som utanför krishanteringssystemet som påverkas när det uppstår störningar i elektronisk kommunikation. Flera 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 insatser för att kunna vidta relevanta åtgärder, som leder till minskade avbrottstider.

PTS och Svenska Kraftnät leder flera samverkansprojekt 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 samverkansformer och rutiner.

7.6.2 Inriktningen är att utveckla en struktur för ömsesidigt informations- och erfarenhetsutbyte

PTS samverkar med SvK, operatörer, branschföreträdare, centrala myndigheter, områdesansvariga myndigheter, kommuner och flera andra aktörer för att utveckla en struktur för ömsesidigt informations- och erfarenhetsutbyte. Samverkan bör leda till att åtgärder ska kunna vidtas koordinerat för att få god effekt såväl för operatörer som för 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.

7.6.3 Exempel på åtgärder

Utveckla samverkan inom sektorn elektronisk kommunikation

- *Nationella telesamverkansgruppen, NTSG*

PTS, TeliaSonera, Skanova, 3, Teracom, TDC Song, Tele2, Telenor, Stokab, Svenska Kraftnät, Banverket, Stadsnätsföreningen och Försvarsmakten ingår i NTSG. Gruppen är en funktion som kan träda i kraft vid allvarliga hot och påfrestningar på samhället i fred i syfte att minimera avbrottstider inom elektronisk kommunikation. Gruppen utgör stommen för att utveckla samverkan med elsektorn.

- Utveckla samverkan mellan Internetoperatörer (ISP:er)

På motsvarande sätt som samverkan sker inom NTSG finns behov av liknande samverkan mellan ISP:er i händelse av svåra störningar i Internettrafiken. Formerna för denna samverkan bör utvecklas.

Samverka mellan sektorerna el och elektronisk kommunikation

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

Genomföra regionala el- och telesamverkansseminarier mellan sektorsansvariga och områdesansvariga aktörer

PTS, SvK, elnätägare, 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.

7.7 Fördjupa det internationella samarbetet

Det internationella samarbetet för att öka säkerheten och robustheten i elektronisk kommunikation 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.

7.7.1 Syftet är att utveckla det internationella perspektivet i planering och utformning av beredskapen för allvarliga hot och påfrestningar på samhället

Elektronisk kommunikation 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 elektronisk kommunikation vid allvarliga hot och 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 inom elektronisk kommunikation för allvarliga hot och påfrestningar på samhället i fred.

7.7.2 Inriktningen är att aktivt delta i internationella fora och utveckla bilaterala kontakter med andra nationer

Det internationella samarbete som under normala förhållanden växer fram mellan såväl operatörer som reglerande myndigheter utgör en av delarna för att skapa säker elektronisk kommunikation också i händelse av kris.

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

7.7.3 Exempel på åtgärder

Utbyta information

Internationella kontakter ger möjligheter till utbyte av information avseende arbetet med säker och robust elektronisk kommunikation. Framförallt gäller det erfarenheter av system och tekniska trender samt hot och konsekvenser för samhället. Informationsteknologiska hot utvecklas snabbt varför utbytet med andra länder i stor utsträckning måste vara av operativ karaktär. För den svenska IT-incidentfunktionen, Sitic, är ett nära samarbete med motsvarande organ dvs. CERTs (Computer Emergency Response Teams) i andra länder av stor betydelse. Sitic har ett väl utvecklat och utnyttjat internationellt nätverk inom CERT-världen. Som utpekad svensk stats-CERT får Sitic snabbt tillgång till information som kan påverka säkerheten för svenska intressenter; Sitic kan även snabbt sprida information till sina motsvarande funktioner i andra länder. I nätverket ingår inte bara CERTar, utan även privata kommersiella och ideella aktörer som har tillgång till information av relevant karaktär.

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.

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 svensk elektronisk kommunikation.

Förbättra förmågan till krishantering

Genom internationellt samarbete och planering förbättras möjligheterna till en effektiv krishantering. (Se även åtgärdsområdet 7.9 Förbättra förmågan till krishantering inom elektronisk kommunikation.)

7.8 **Förbättra förmågan till krisledning inom elektronisk kommunikation**

Åtgärder bör vidtas för att skapa en beredskap att snabbt avhjälpa störningar och avbrott. Det måste finnas tillgång till personal, reservutrustningar och transportabla system som kan användas i svåra situationer, samt att genom planering och övning skapa en handlingsberedskap för att kunna agera i kriser.

7.8.1 Syftet är att förbättra förmågan till krisledning inom sektorn elektronisk kommunikation

Det kommer alltid att finnas risker för störningar och avbrott i elektronisk kommunikation som snabbt måste kunna avhjälpas. För detta behövs en effektiv krisledning som verkar för att avbrotten blir så korta som möjligt och får en begränsad omfattning.

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

7.8.2 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 krisledningsarbetet i eget nät.

7.8.3 Exempel på åtgärder

Genomföra övningar

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

Utbilda personal

Tillgången till kompetent personal är av avgörande betydelse för möjligheten att hantera krissituationer. Individanpassad utbildning i krishantering för sektorns aktörer är en del i arbetet.

Införskaffa reservutrustning

Reservutrustning och mobila system som behövs vid krishantering är något som måste anskaffas innan en kris uppstår.

Utveckla internationellt samarbete

I och med att elektronisk kommunikation 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.

7.9 Öka effekten av robusthetsåtgärder i näten

Effekten av robusthetsåtgärder 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.

7.9.1 Syftet är att effektivisera de robusthetshöjande åtgärderna och utveckla samverkan med andra delar i samhället

Det sker idag en mycket snabb teknisk utveckling inom området elektronisk kommunikation. 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.

7.9.2 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.

7.9.3 Exempel på åtgärder

Utföra praktiska tester

Genom praktiska tester av elektronisk kommunikation 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.

Medverka i uppföljningsstudier

Då större störningar inträffar ska 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

8 Grunder för prioritering av insatser

Grunder för prioritering av insatser utgörs av två övergripande målsättningar

- dels ska en nivå av robusthet som motsvarar samhällsviktiga användares och samhällets krav skapas i infrastrukturen och verksamheten för elektronisk kommunikation,
- dels ska det skapas förutsättningar för att samhällsviktiga användare och totalförsvarets aktörer ska kunna verka i händelse av en kris eller i en beredskapssituation.

Åtgärder som leder till ökad uthållighet och kortare avbrottstider ska prioriteras.

Verksamheten ska bedrivas i nära samverkan, i så kalla privatoffentlig samverkan mellan PTS och näringslivet. Arbetet ska präglas av en respektfull och förtroendeingivande dialog där såväl statens som aktuell operatörs behov ska kunna tillgodoses. Arbetet ska bedrivas så att möjligheter kan tas tillvara när de uppstår. Ett sådant arbetssätt leder till kostnadseffektiv nyttjande av såväl statens som näringslivets medel och resurser.

PTS ska vara drivande för att öka den generella krisledningsförmågan och robustheten i samhället med kraftsamling i den egna sektorn. I och med att elektronisk kommunikation berör stora delar av samhället erhålls per automatik effekt även i andra sektorer. Även om arbetet till sin natur präglas av sektorsöverskridande arbete ska PTS också verka för direkt tvärsektoriell samverkan där så är lämpligt.

PTS ska ha ett nära samarbete med andra sektor som etablerat fasta former för privatoffentlig samverkan. Exempelvis kraftförsörjningens Elsamverkansledningar, ELS.

PTS skall verka för att öka förståelsen för det gränsöverskridande beroendet av elektronisk kommunikation.

Arbetet skall genomföras ur såväl ett globalt, nationellt som underifrånperspektiv.

Medlen ska nyttjas på ett kostnadseffektivt sätt. Där behov uppstår och det inte finns några kommersiella grunder för åtgärderna ska staten svara för finansiering. Där det finns såväl kommersiella behov som samhällsviktiga

behov ska kostnaderna fördelas mellan stat och operatör. Hur fördelningen sker får avgöras från fall till fall. Där behovet löses på kommersiella grunder skall operatören bära sina egna kostnader.

Samverkansformer ska etableras och formaliseras för att säkerställa långsiktighet och ökad effektiviteten av arbetet.

Ett stort antal aktörer inom sektorn är nystartade företag som i flera fall inte har tillräcklig kunskap av verksamheten för att svara upp mot samhällets krav på robusthet. Det robustethöjande arbetet måste därför bedrivas så att också generella stödinsatser på grundläggande nivåer kan genomföras. Dessa satsningar är ofta insatser som kan nyttjas av flera aktörer. Exempel på sådana åtgärder kan vara framtagande av rekommendationer, utbildningar och instruktioner.

Resultatet av vidtagna åtgärder ska så långt som möjligt kunna användas i fredstid för att säkerställa funktion i händelse av krig.

PTS skall delta i internationella samarbetsorganisationer och där så är lämpligt lyfta fram det svenska robusthets och säkerhetsarbetet. Genom att visa på ”best practice” ska PTS söka påverka robusthets- och säkerhetsarbetet i internationella sammanhang.

Ordlista

BGP - Border Gateway Protocol, ett protokoll som används för spridning av routinginformation mellan Internetoperatörer.

DNS – Domain Name System. Ett adresseringssystem för Internet.

DNSSEC – DNS Security Extensions, en standard för att med kryptografiska metoder garantera spårbarhet och informationen inte ändrats på vägen

GLU – System för gemensam lägesuppfattning.

ICANN – Internet Corporation for Assigned Names and Numbers, en privaträttslig organisation som förvaltar vitala delar av DNS och IP-adresser

IANA – Internet Assigned Numbers Authority, ansvarar operativt på uppdrag av ICANN att förvalta och dela ut IP-adresser

IETF – Internet Engineering Task Force, en organisation som tar fram standarder i form av RFC:er (Request for Comments)

IMS – IP Multimedia Subsystems, En standard som möjliggör tal och multimedia över mobilnät och fasta nät med hjälp av IP-teknik

IP-baserade nät – Paketförmedlande nät som använder sig av Internet Protocol, RFC791

IP-baserad telefoni – Telefoni som någon gång går över ett IP-baserat nät.

IPX - IP Packet eXchange, en nyutvecklad tjänst baserad på IP-protokollet, men med den skillnaden att kvaliteten garanteras hela vägen mellan mottagare och sändare

ISP – Internet Service Provider, aktör som tillhandahåller anslutning till Internet och som förmedlar trafik över Internet.

IXP – IP Packet Exchange, knutpunkt med funktioner för utbyte av IP-trafik mellan Internet-/IP-operatörer

Konvergens – Utveckling från att enskilda typer av tjänster (TV, radio, telefoni, etc.) levereras genom specifika nät till dedicerade terminaler till att

flera olika typer av tjänster kan levereras till flera olika typer av terminaler genom ett gemensamt nät.

LEK – Lagen (2003:389) om elektronisk kommunikation.

NGN – Nästa generations nät. En viktig del i begreppet är att elektroniska kommunikationsnät utvecklas till att bli helt eller delvis IP-baserade och kan tillhandahålla många tjänster såsom telefoni, data och video via olika typer av accessnät.

NTSG – Nationell telesamverkansgrupp.

Optisk fiber – Fiberbaserad infrastruktur. Optisk fiber är en tunn gasledning av kiseldioxid (glas) som överför information via ljus istället för via elektroniska signaler som sker i en kopparledning. Kan finnas i hela eller delar av elektroniska kommunikationsnät.

Resolver - Namnservrar i DNS som ställer DNS-frågor till andra namnservrar för att t.ex översätta namn till adress som en servicefunktion åt slutanvändare

Robusthet - förmåga att fungera trots svåra påfrestningar.

SITIC – Sveriges IT-incidentcentrum (del av PTS).

SS7 - Signalling System 7. En signaleringsstandard för att sätta upp kretskopplad förbindelse.

SIP – Session Initiating Protocol. En signaleringsstandard för att koppla upp paketfördelad förbindelse.

UMTS – Universal Mobile Telecommunications System. En standard för tredje generationens mobiltelefoni.

Zon - del av en domän som en viss namnsverradministratör/operatör är ansvarig för, exempelvis är PTS ansvarig för zonen pts.se som är en del av domänen .se.