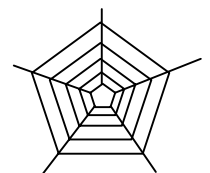


Svante Barck-Holst

# Nationellt säkerhetsarbete inom samhällsviktig infrastruktur





TOTALFÖRSVARETS FORSKNING SINSTITUT

Försvarsanalys  
172 90 Stockholm

FOI-R--1553--SE

Januari 2005

ISSN 1650-1942

**Underlagsrapport**

Svante Barck-Holst

# Nationellt säkerhetsarbete inom samhällsviktig infrastruktur



<b>Utgivare</b> Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	<b>Rapportnummer, ISRN</b> FOI-R--1553--SE	<b>Klassificering</b> Underlagsrapport
	<b>Forskningsområde</b> 1. Analys av säkerhet och sårbarhet	
	<b>Månad, år</b> Januari 2005	<b>Projektnummer</b> E1740
	<b>Delområde</b> 13 Stöd till säkerhet och beredskap	
	<b>Delområde 2</b>	
<b>Författare/redaktör</b> Svante Barck-Holst	<b>Projektledare</b> Georg Fischer	
	<b>Godkänd av</b> Staffan Molin	
	<b>Uppdragsgivare/kundbeteckning</b> Krisberedskapsmyndigheten	
	<b>Tekniskt och/eller vetenskapligt ansvarig</b> Svante Barck-Holst	
<b>Rapportens titel</b> Nationellt säkerhetsarbete inom samhällsviktig infrastruktur		
<b>Sammanfattning (högst 200 ord)</b> <p>I rapporten görs en genomgång av hur man i Sverige på nationell nivå har arbetat med sårbarhetsfrågor som rör elförsörjning, telekommunikationer samt informationsförsörjning under de senaste 40 åren.</p> <p>För var och en av de tre områdena redovisas en översiktlig historik rörande systemens utveckling och förändring i sårbarhet. Detta som en bakgrund till en genomgång av vilka åtgärder som vidtagits på nationell nivå för respektive område. I denna genomgång redovisas bedömningar som gjorts och inriktning på åtgärder som valts.</p> <p>Slutligen identifieras några viktiga faktorer som påverkat hanteringen av säkerhetsarbetet på nationell nivå inom de olika systemen. Exempel på faktorer som diskuteras är:</p> <ul style="list-style-type: none"> <li>- elektronikens och dators utveckling</li> <li>- hot om angrepp med IT-vapen</li> <li>- hot från sabotageförband</li> <li>- hot från luftburna precisionsvapen</li> <li>- det kalla krigets slut</li> <li>- marknadsreformer</li> </ul>		
<b>Nyckelord</b> Telekommunikationer, elförsörjning, informationsförsörjning, samhällsviktig infrastruktur, ADB-säkerhet		
<b>Övriga bibliografiska uppgifter</b>	<b>Språk</b> Svenska	
<b>ISSN</b> 1650-1942	<b>Antal sidor:</b> 49 s.	
<b>Distribution enligt missiv</b>	<b>Pris:</b> Enligt prislista	



<b>Issuing organization</b> FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	<b>Report number, ISRN</b> FOI-R--1553--SE	<b>Report type</b> Base data report
	<b>Programme Areas</b> 1. Security, safety and vulnerability analyses	
	<b>Month year</b> January 2005	<b>Project no.</b> E1740
	<b>Subcategories</b> 13 Support to Security, Safety and Preparedness	
	<b>Subcategories 2</b>	
<b>Author/s (editor/s)</b> Svante Barck-Holst	<b>Project manager</b> Georg Fischer	
	<b>Approved by</b> Staffan Molin	
	<b>Sponsoring agency</b> Swedish Emergency Management Agency	
	<b>Scientifically and technically responsible</b> Svante Barck-Holst	
<b>Report title (In translation)</b> Critical Infrastructure Protection - A Swedish Retrospective		
<b>Abstract (not more than 200 words)</b> <p>The report explores how Sweden during the last 40 years, at a national level, has handled vulnerability issues concerning infrastructures for electric power supply, telecommunication and information technology. For each infrastructure there is an historic overview of the development of the systems and their vulnerabilities. Measures taken at a national level for each of the infrastructures is then presented. Finally the report identifies important factors that has influenced the choice of measures. Examples are:</p> <ul style="list-style-type: none"> <li>- the development of electronics and computers</li> <li>- threat of electronic attacks</li> <li>- threat from military sabotage units</li> <li>- threat of precision bombing</li> <li>- the end of the Cold War</li> <li>- market reforms</li> </ul>		
<b>Keywords</b> telecommunication, power supply, information security		
<b>Further bibliographic information</b>	<b>Language</b> Swedish	
<b>ISSN</b> 1650-1942	<b>Pages</b> 49 p.	
	<b>Price acc. to pricelist</b>	





## Innehållsförteckning

Innehållsförteckning .....	1
1 Inledning.....	3
1.1 Bakgrund .....	3
1.2 Syfte och mål.....	3
1.3 Avgränsningar .....	3
1.4 Metod .....	4
1.5 Läsanvisning.....	4
2 Telekommunikationer .....	5
2.1 System .....	5
2.2 Sårbarheter .....	6
2.3 Nationella satsningar .....	8
2.3.1 1970-talet – Ett telenät rustat för krig .....	8
2.3.2 1980-talet – Digitalisering ger nya möjligheter .....	10
2.3.3 1990-talet – Nya tider och marknadsreformer .....	12
2.3.4 2000-talet – IT och konvergens.....	15
3 Elförsörjning.....	17
3.1 System .....	17
3.2 Sårbarheter .....	18
3.3 Nationella satsningar .....	19
3.3.1 1970-talet och dessförinnan .....	19
3.3.2 1980-talet – Sabotagehot och störning .....	21
3.3.3 1990-talet – Organisatoriska förändringar .....	22
3.3.4 2000-talet – Fokus på samhällets elberoende.....	26
4 Informationsförsörjning .....	29
4.1 System .....	29
4.2 Sårbarheter .....	30
4.3 Nationella satsningar .....	31
4.3.1 1970-talet – ADB-säkerhet, en ny fråga.....	32
4.3.2 1980-talet – Tekniken mognar .....	35
4.3.3 1990-talet – Internet: möjligheter och problem.....	38
4.3.4 2000-talet – Myndighetsansvar fördelas .....	41
5 Slutord.....	43
Referenser.....	45



# 1 Inledning

## 1.1 Bakgrund

Totalförsvarets främsta uppgift var länge att vara så förberett för *kriget* att det verkade fredsbevarande. I och med det kalla krigets slut förändrades den hotbild som Sverige sedan andra världskriget förberett sig för. Det militära försvarets betydelse minskade. Internationellt skedde förändringar och exempelvis NATO började utgå från en breddad hotbild vilket också noterades i Sverige<sup>1</sup>. I USA uppmärksammades sårbarheterna i den samhällsviktiga infrastrukturen i slutet av 1990-talet<sup>2</sup> och det civila samhällets sårbarhet demonstrerades med all tydlighet den 11 september 2001. Det kan därför verka som att sårbarheten och säkerheten i den samhällsviktiga infrastrukturen är en relativt nyväckt fråga. Men i Sverige har det under flera decennier bedrivits ett omfattande arbete inom området.

Under lång tid har det framhållits att ett robust och uthålligt fredssamhälle är en viktig förutsättning för Sveriges förmåga att stå emot olika hot mot den nationella säkerheten. Utöver tillgången till olika förnödenheter och insatsvaror så har samhällets behov av energiförsörjning, telekommunikationer etc. funnits med i planeringen. I takt med att datoriseringen fått en allt större betydelse för samhällets funktion så har även de IT-relaterade sårbarhetsfrågorna lyfts fram, under lång tid under beteckningen ADB-säkerhet. Den tidiga prioriteringen av försörjningsfrågorna har bland annat lett till att mycket av samhällets säkerhetsarbete är institutionaliserat och kan idag återfinnas i exempelvis författningar och tekniska standarder. Ny teknik och olika samhällsförändringar gör dock att man ständigt måste ompröva de strategier och åtgärder som man väljer för att minska samhällets sårbarhet.

I samband med en förändrad hotbild och en tyngdpunktsförskjutning i tänkandet kring den nationella säkerheten finns det en risk att de kunskaper och erfarenheter som ackumulerats om säkringen av samhällsviktig infrastruktur går förlorad eller inte beaktas i dagens arbete. Mer eller mindre abrupta personella generationsskiften inom centrala myndigheter och andra organisationer kan också göra att de strategier och åtgärdsförslag som skall hantera framtidens säkerhetsproblem förbiser viktiga "historiska" lärdomar.

I takt med den ökande graden av samverkan med andra länder kring frågor om säkringen av samhällsviktig infrastruktur finns det ett behov av att kunna ge en tydlig beskrivning av den svenska traditionen inom området.

## 1.2 Syfte och mål

Syftet med denna studie är att klarlägga och beskriva hur vi i Sverige har arbetat med sårbarhetsfrågor som rör elförsörjning, telekommunikationer samt informationsförsörjning.

Målet med arbetet är att kunna ge en samlad bild av hur vi på nationell nivå har studerat frågan, vilka bedömningar som gjorts och vilken inriktning på åtgärderna man valt. I förlängningen skall arbetet bidra till en allmän tradering av erfarenheterna från tidigare arbete med säkring av samhällsviktig infrastruktur.

## 1.3 Avgränsningar

Under tiden från slutet av 1800-talet fram till och med 1960-talet sker enorma tekniska framsteg och stora samhällsförändringar. Sverige industrialiseras, el och telesystem byggs upp och mognar. Sverige anpassar sig efter andra världskriget till det kalla krigets villkor och står

<sup>1</sup> Proposition 1995/95:12 Totalförsvaret i förnyelse

<sup>2</sup> The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 22 maj 1998

som bäst rustat runt 1960. ADB och informationsförsörjning i den tekniska kontext som är intressant för denna studie tar form på 1960-talet. De system som studeras börjar då på allvar bli oundgängliga i det svenska samhället. Den genomgång av satsningar på samhällsviktig infrastruktur som genomförs tar därför sitt avstamp i 1960-talet och fortsätter fram till sekelskiftets första år. Denna tidsperiod karakteriseras av en snabb teknisk utveckling samt stora säkerhets- och inrikespolitiska förändringar, samtidigt som den ligger så pass nära i tiden att man kan se en direkt koppling till dagens situation. Det är dock värt att notera att det har vidtagits beredskapsåtgärder för att säkra elförsörjningen sedan 1930-talet och krigsskyddsåtgärder för telekommunikationerna sedan 1940-talet.

## **1.4 Metod**

Inledningsvis genomfördes litteraturstudier på bred front liksom intervjuer med personer med lång erfarenhet av frågor som rör den tekniska infrastrukturens säkerhet och beredskap. Därefter har arbetet inriktats på att leta fram de satsningar som redovisats i regeringens propositioner, främst de som berör olika försvarsbeslut. Detta material har dessutom kompletterats med rapporter och planer från ansvariga myndigheter.

## **1.5 Läsanvisning**

Rapporten är indelad i fyra kapitel där kapitel 1 Inledning ger en bakgrund till arbetet. Därefter avhandlas de tre områdena telekommunikationer, elförsörjning och informationsförsörjning var för sig i kapitel 2, 3 och 4 respektive.

Strukturen i dessa tre kapitel är identisk. De inleds med ett avsnitt om systemets historiska utveckling i Sverige. Fokus är framförallt på tekniska förändringar och framsteg, men det redogörs även till en viss del hur samhällets utveckling har påverkat systemen.

Därefter följer ett avsnitt i vilket vi redogör för hur sårbarheten i systemet har förändrats med tiden. Sårbarheten är en funktion av systemens tekniska egenskaper och tillkortakommanden, de vapen och hot som kan utnyttjas för att störa systemen samt de konsekvenser som uppstår för samhället om det betraktade systemet drabbas av störningar.

Idén med dessa två inledande avsnitt om system och sårbarheter är att ge en bred och översiktlig bakgrund som förberedelse inför det sista avsnittet i vilket vi redogör för det säkerhetsarbete som bedrivits på nationell nivå för respektive system. Genomgångarna i dessa avsnitt görs kronologiskt baserat på propositioner, programplaner, rapporter och andra relevanta dokument.

## 2 Telekommunikationer

Infrastrukturen för telekommunikationer omfattar en mängd tekniska system för överföring av ljud, text, bild, data eller information i övrigt. I detta kapitel diskuterar vi också telekommunikationerna ur detta breda perspektiv. Med detta vida anslag kan man tycka att Internet och dess utveckling skulle behandlas i detta kapitel, vi har dock valt att låta detta behandlas i kapitlet Informationsförsörjning istället.

I detta kapitel presenteras först systemen för telekommunikation och hur dessa har utvecklats. Därefter följer en beskrivning av hur sårbarheten har förändrats under de senaste 40 åren. Slutligen görs en genomgång av hur arbetet med dessa frågor har bedrivits på nationell nivå.

### 2.1 System

Efter andra världskriget fanns det i Sverige drygt 1,2 miljoner telefonapparater. Svenska Telegrafverket hade på 1920-talet påbörjat en automatisering av växelsystemen och 1945 var cirka 700 000 av telefonapparaterna anslutna till helautomatiska växelstationer. Det skulle ta ända fram till juni 1972 innan den sista manuella växelstationen ersattes och telenätet var helautomatiserat. Under denna tidsperiod ökade antalet telefonapparater till knappt 4,7 miljoner. Ytterligare 15 år senare var antalet telefonapparater 7 miljoner.

Överföringskapaciteten var länge begränsande och det arbetades kontinuerlig på förbättring och utbyggnad av telefonnätet. Koaxialkabeln som fick sitt genombrott i Sverige 1947<sup>3</sup> var länge dominerande för överföring av samtal på stora avstånd. På 50-talet kommer även radiolänktekniken som i många avseenden kompletterade koaxialkabeln.

Under 1970-talet investerade Televerket inte i någon större utsträckning i den kopplings-tekniska utrustningen. Den digitala tekniken var ännu inte riktigt mogen. Men med Ericssons AXE-teknik lossnade det och 1980 installeras den första AXE-växeln i Sverige. Det dröjde ytterligare 18 år innan det svenska telenätet var helt digitaliserat. Den digitala tekniken har medfört ökade möjligheter att erbjuda olika typer av tjänster, dessutom utökades den tillgängliga kapaciteten i näten.

Ytterligare en revolution påbörjas med införandet av optiska fibrer i mitten av 80-talet. Det hade då uppstått en kapacitets- och kvalitetskris i det svenska telenätet vilket påskyndade införandet av optokabel<sup>4</sup>. Optisk överföring har stor kapacitet och kablarna kan utformas med små dimensioner vilket ger låg vikt. Dessutom är det möjligt att tillverka helt metallfria kablar okänsliga för elektriska störningar.

Den snabba tekniska utvecklingen och förändringar i politisk inställning försvagade under 80-talet Televerkets de facto monopol som enda aktör på den svenska telemarknaden<sup>5</sup>. Telemarknaden reformerades och 1993 bolagiserades Televerket och blev Telia. Även om Telia under större delen av 90-talet har varit dominerande på telemarknaden så har ett stort antal nya operatörer och nätägare etablerat sig. Det innebär att det idag finns ett flertal aktörer som kan erbjuda olika former av teletjänster i egna eller hyrda nät. Under 90-talet började man även införa så kallad SDH-teknik. Denna teknik är baserad på en internationell standard för digital transmission och innebär framför allt ökade möjligheter till styrning och övervakning av näten.

<sup>3</sup> Svenska telegrafverket : historisk framställning. Bd 6, Telefon, telegraf och radio 1946-1965

<sup>4</sup> Svenska telegrafverket : historisk framställning. D. 7, Från myndighet till bolag: 1966-1993

<sup>5</sup> Se exempelvis Offentlighetens nya rum – Teknik och politik i Sverige 1969-1999, Lars Ilshammar, Örebro Universitet

Trevande försök med mobiltelefoni gjordes redan på 50-talet. Det är dock först med NMT-systemet som mobiltelefonin tar riktig fart. Ett nordiskt mobiltelefonisystem NMT 450 introducerades 1981 och följdes av NMT 900 sex år senare. Skillnaden mellan vanlig telefoni och mobiltelefoni är huvudsakligen att mobilnätets accessnät är trådlöst och att det mobila nätet behöver funktionalitet för att lokalisera och identifiera abonnenterna. NMT 450 använder sig av radiofrekvenser i 450 MHz bandet och NMT 900 använde sig av 900 MHz bandet. Låga frekvenser har längre räckvidd och man kan alltså med få basstationer täcka ett stort område vilket är en fördel i glest befolkade områden.

I början av 90-talet kom så GSM, det stora genombrottet för mobil telefoni. Nu var inte Televerket längre ensamma om telefoni på den svenska marknaden. Comviq GSM AB och Europolitan startade båda kommersiell drift av GSM i september 1992 följda av Televerket i november 1992. GSM systemet som är helt digitalt bygger på en internationellt accepterad standard och telefonerna går att använda i många länder. GSM-nätet använder sig av radiofrekvenser runt 900 MHz, 1800 MHz och 1900 MHz. NMT 900 lades därför ner 2000. NMT 450 drivs fortfarande men tillståndet går ut 2007.

Sedan slutet av 90-talet har gränsen mellan olika tekniker, marknader, tjänster och utrustning för kommunikation och information allt mera suddats ut, något som brukar benämnas konvergens<sup>6</sup>.

## 2.2 Sårbarheter

Sårbarheterna i telefonisystemen förändras naturligtvis i takt med att tekniken utvecklas. Nya lösningar innebär att vissa sårbarheter elimineras medan andra tillkommer. Likaså påverkas sårbarheten av förändringar i de hot som riktas mot systemen. Nya vapen med högre precision eller speciellt inriktade på vissa systemegenskaper ökar sårbarheten medan nya motmedel eller tekniska lösningar kan minska sårbarheten. Synen på ett systems sårbarheter påverkas även av samhällets beroende av systemet och de konsekvenser som kan följa av att en sårbarhet utnyttjas.

Teknikutvecklingen och övergången från elektronmekanik till avancerad elektronik har medfört att de komponenter som ingår i telekommunikationssystemen har fått allt större kapacitet och tillförlitlighet. Enskilda stationer kan hantera allt fler abonnenter och en optisk kabel kan förmedla väsentligt fler samtal än en kopparkabel. Samtidigt innebär detta att sammanbrott i en enskild komponent kan drabba mer trafik och fler abonnenter än tidigare.

Datorisering har medfört en betydligt ökad möjlighet för centralt ledd och i många delar automatiserad övervakning och styrning. Detta leder till att man har en betydligt bättre kontroll över systemen. Man får snabbare reda på när något gått fel och fel kan åtgärdas mycket snabbt, ibland omedelbart genom exempelvis automatisk inkoppling av reservsystem. Man har även en förbättrad överblick över systemets status och en möjlighet att prioritera insatser då större skador inträffar. Denna centralisering och möjlighet att fjärrstyra delar av telenäten medför även en ökad sårbarhet då enskilda personers misstag eller medvetet illasinnade handlingar kan få stora konsekvenser.

Datorisering och automatisering har även medfört att man kunnat reducera mängden personal som krävs för att underhålla systemet. Vid större störningar finns det därför mindre personal att tillgå för att åtgärda de problem som uppstår. Så även om man kan hantera mindre störningar snabbt kan större störningar eventuellt orsaka längre avbrott.

Ett sista exempel på hur teknikutvecklingen påverkat sårbarheten är införandet av mobiltelefoni. Genom att ersätta kablarna i accessnätet med radioöverföring har man eliminerat en

<sup>6</sup> SOU 1999:55 Konvergens och förändring – Samordning av lagstiftningen för medie- och telesektorerna

fysisk komponent och således en möjlig sårbar punkt. Men naturligtvis finns det möjligheter att störa radiovågor.

Hur har då de direkta hot som kan riktas mot telekommunikationerna förändrats? Om vi börjar med att studera slumpmässiga hot så kan man inte säga att risken för olyckor och mänskliga misstag har ökat. Här är det snarare teknikutvecklingen som bidrar till att påverka sårbarheten. Däremot finns det ju de som menar att växthuseffekten leder till ett våldsammare väder, ett allvarigare hot och alltså en ökad sårbarhet.

När det gäller antagonistiska hot kan man dock se en tydlig utveckling som har lett till en ökad sårbarhet. Möjlig precision vid angrepp genom luften har genom den militärtekniska utvecklingen blivit mycket hög. En angripare med kunskap om vilka delar av systemet som skall angripas kan åstadkomma stor skada. Så kallade HPM<sup>7</sup>-vapen, som kan generera starka elektromagnetiska pulser och på så sätt slå ut elektroniska komponenter har utvecklats. Dessa hot påverkar sårbarheten men har även mötts av motåtgärder som exempelvis bergrumsförläggning av vitala komponenter.

Ytterligare hot som tillkommit är IT-hot i form av logiska attacker mot mjukvarubaserade system. Påverkan på sårbarheten beror i detta fall även på teknikutvecklingen som ju möjliggjort störningar från denna typ av hot.

Slutligen påverkas även synen på telekommunikationernas sårbarhet av samhällets utveckling. Under 1990-talet har trenden varit att reformera och konkurrensutsätta marknader som tidigare dominerats av stora statliga bolag. Televerket blev Telia och det dök upp en mängd konkurrenter på telemarknaden. Bland annat medförde detta att det dök upp flera alternativa mobiltelefonisystem med delvis separat infrastruktur och därmed ett minskat beroende av ett enskilt system.

Den nya marknadssituationen under 90-talet medförde också att det blev viktigt för alla aktörer att kunna erbjuda teletjänster till konkurrenskraftiga priser. Ett tillvägagångssätt har varit att köpa drift och underhåll på entreprenad och på så sätt undvika att sitta med underutnyttjad personal utan istället kunna köpa in extra kapacitet när det är befogat. Många operatörer förlitar sig därför på samma entreprenörer för att kunna avhjälpa fel vid eventuella störningar. I en situation med stora, samtidiga skador på telesystemen skulle det kunna uppstå brist på kompetent reparationspersonal. Personalbrist i en krissituation var visserligen inte omöjligt under tidigare perioder heller men på en konkurrensutsatt marknad finns ett tryck på att minska kostnaden för extra säkerhet i form av överkapacitet.

Kostnadsjakt i kombination med en snabb teknikutveckling har även betytt en allmänt minskad lagerhållning. Under det kalla kriget försökte den svenska staten genom ÖEF och senare ÖCB att kompensera för detta genom att betala för beredskapslagring. Med det kalla krigets slut har de scenarion med skymningslägen, avspärning och invasion av Sverige som tidigare varit aktuella blivit mindre trovärdiga. Någon omfattande beredskapslagring av elektroniska komponenter förekommer därför inte längre. Däremot kvarstår andra trovärdiga scenarier som skulle kunna resultera i komponentbrist, exempelvis att en dominerande internationell producent av komponenter får leveransproblem på grund av naturkatastrofer, råvarubrist, tekniska problem eller oroligheter i den världsdelen där komponenterna produceras.

Avslutningsvis är det värt att påpeka att samhället idag är mycket mer beroende av fungerande telekommunikationer än tidigare. Idag räknar vi i Sverige med att ha konstant tillgång till väl fungerande telekommunikationer var i landet vi än befinner oss. Tillförlitligheten är mycket hög och benägenheten att planera för alternativ till

---

<sup>7</sup> HPM - High Power Microwave

telekommunikationer är därför låg. Detta är dock en faktor som påverkar samhällets sårbarhet snarare än telekommunikationernas.

## **2.3 Nationella satsningar**

I televerkets nät har det ända sedan 1940-talet vidtagits krigsskyddsåtgärder bland annat i form av anordnande av reservtelefonstationer och anskaffning av mobil ersättningsutrustning.<sup>8</sup> Dessa åtgärder har finansierats via anslag från försvarsbudgeten efter anvisningar från riksdagen. Utöver detta har televerket vidtagit egna åtgärder riktade mot fredstida störningar finansierade inom ramen för den egna driften.

### **2.3.1 1970-talet – Ett telenät rustat för krig**

#### **1970 års försvarsutredning**

Vid en föredragning för 1970 års försvarsutredning redovisade Televerket<sup>9</sup>:

”Sedan omkring 15 år tillbaka har man i samband med den av fredsmässiga skäl betingade utbyggnaden av televerkets anläggningar vidtagit, åtgärder för att bland annat

- göra telenätet, - främst fjärrnätet - allt mer maskformigt,
- ge nya, viktigare linjeanläggningar - kablar och i radiolänkar - sådan sträckning att särskilda riskområden undvikas,
- vid nybyggnad av särskilt viktiga stationsanläggningar ge dessa en från särskilda riskområden, t ex större städer undandragen lokalisering samt
- utföra i princip alla nya hus för större och viktigare stationsanläggningar med visst byggnadstekniskt skydd.

För att säkerställa de tidigare nämnda krigsviktiga telefonabonnenternas förbindelser har vidare en plan uppgjorts för modernisering av ett sedan länge befintligt men i dag tekniskt föråldrat landsomfattande reservtelefonnät med manuellt betjänade reservtelefonstationer i skyddade lokaler. Denna modernisering har nyligen startats.

För att eliminera risken för att det automatiska telefonnätet blir blockerat vid onormala trafiksituationer har ett trafikbegränsningssystem utvecklats, som fungerar så att icke krigsviktiga abonnenter vid behov automatiskt avstänges till förmån för de krigsviktigas trafik. Införandet av detta system har icke påbörjats.

Härutöver har viss mobil eller transportabel reservutrustning anskaffats i mycket begränsad omfattning.

De särskilda anslag som Kungl Maj:t ställt till förfogande för åtgärder av ovan angivet slag har för den senaste 10-årsperioden uppgått till totalt 80 miljoner kronor.”

Televerkets bedömning 1971 var att läget i fråga om åtgärder för att säkerställa driften i krig inte var tillfredsställande. De allvarligaste bristerna ansågs vara

<sup>8</sup> Enligt proposition 1981/82:102 om säkerhets och försvarspolitikerna samt totalförsvarets fortsatta utveckling

<sup>9</sup> Televerkets uppgifter för totalförsvaret, Föredragning för 1970 års försvarsutredning



- att modernisering av reservtelefonnätet inte hade kommit till stånd,
- att trafikbegränsningssystemet inte var infört samt
- att tillgången till transportabel och mobil utrustning var för liten.

Televerket redovisade för försvarsutredningen följande riktlinjer för det fortsatta arbetet:

1. Åtgärder för att öka driftsäkerheten i det ordinarie nätet i form av spridning och utflyttning av anläggningar bör fortsätta.
2. Nyttillkommande fredsmässiga anläggningar bör ges visst skydd mot vapenverkan.
3. Den modernisering av reservtelefonnätet som nyligen startats bör fullföljas så snabbt som möjligt. Samtidigt bör på sikt övergång till ett mindre personalkrävande reservsystem övervägas och utredas.
4. Det planerade systemet för automatisk begränsning av den icke krigsviktiga telefontrafiken bör snarast möjligt införas.
5. Anskaffningen av mobila och transportabla reservutrustningar bör fortsätta om möjligt i ökad omfattning.
6. Särskilda åtgärder bör övervägas för att säkerställa telex- och datanäten.
7. Särskilda åtgärder bör också övervägas för att säkerställa förbindelserna med utlandet.
8. Särskilda åtgärder bör vidtas för att säkerställa de exklusiva förbindelser för totalförsvaret som anordnas i televerkets nät.

### **Proposition 1976/77:74 om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling**

Televerket var 1976 den enda aktör som tillhandahöll telekommunikationer i Sverige. Televerket hade bland annat som uppgift att planera verksamhet i krig och under beredskap så att skilda totalförsvargrenars behov av telekommunikationer kunde tillgodoses. I totalförsvarsammanhang sorterade Televerket under rubriken ”Övrigt totalförsvär: programmet Ledning m.m.”, vilket låg under kommunikationsdepartementets verksamhetsområde.

Som underlag för propositionen hade Televerket presenterat en programplan för perioden 1977/78-1981/82. Denna programplan var enligt de anvisningar som gavs inriktad mot att förstärka de mest avgörande funktionernas uthållighet, vilket innebar satsningar på reservtelefonstationer, transportabel utrustning samt skydd för telex- och datanät. Den föreslagna budgetramen var på 6 miljoner kronor per år, men Televerket ville ha en budgetram på 10 miljoner kronor per år för att hinna bygga ut i acceptabel takt.

I förarbeten till propositionen konstaterade 1974 års Försvarsutredning i sina betänkanden Säkerhetspolitik och totalförsvär<sup>10</sup> och Totalförsvaret 1977-82<sup>11</sup> att samhällets beroende av telekommunikationer liksom känsligheten för störningar av dessa skulle komma att öka. Detta motiverade enligt försvarsutredningen att åtgärder genomfördes i en något ökad takt. Försvarsutredningen konstaterade dessutom att totalförsvarets samband i krig inom en över-skådlig framtid skulle komma att bygga på Televerkets nät. Försvarsutredningen ville betona betydelsen av att uppmärksamma frågor om trafikbegränsning i kris och krig. Dessutom ansåg man att det borde finnas tillräckligt med transportabel reservmateriel för att kunna ersätta de viktigaste förbindelserna vid krigsskador.

<sup>10</sup> SOU 1976:5 Säkerhetspolitik och totalförsvär

<sup>11</sup> SOU 1977:1 Totalförsvaret 1977-81

### 2.3.2 1980-talet – Digitalisering ger nya möjligheter

#### **Proposition 1981/82:102 om säkerhets- och försvarspolitikerna samt totalförsvarets fortsatta utveckling**

Organisatoriskt har inget förändrats på de fem år som gått sedan försvarspropositionen 1976/77:74. Televerket har samma uppgift avseende planering för beredskap och krig och redovisas inriktningen fortfarande av kommunikationsdepartementet under rubriken "Övrigt totalförsvaret: programmet Ledning m.m."

Inför försvarsbeslutet hade Televerket tagit fram en verksamhetsplan för åren 1982/83-1986/87 avseende verkets försvarsberedskap. Anvisningarna var att förstärka krigsuthålligheten hos verkets anläggningar.

Televerket har vid denna tidpunkt påbörjat övergången till digitala system och detta avspeglar sig i propositionen och dess förarbeten. I sitt betänkande Totalförsvaret 1982/87<sup>12</sup> konstaterar 1978 års försvarskommitté att sårbarheten hos telefunktionen har ökat då tekniken blivit mer komplicerad och koncentrerad<sup>13</sup>. Kommittén anser att det är angeläget att krigsskyddsåtgärder även genomförs för de digitala systemen och att utbyggnad av digitala reservstationer bör ske jämsides med den fredstida uppbyggnaden. Att behålla de gamla manuella reservstationerna anses medföra stora kostnader och tekniska problem. Dessutom vill kommittén införa system för telefonalarmering i de nya stationerna.

Propositionen konstaterar att Totalförsvaret till stor del är beroende av Televerkets nät och stödjer uppbyggandet av ett automatiskt reservsystem som i så stor utsträckning som möjligt skall vara baserat på de fredsmässiga resurserna.

#### **Proposition 1986/87:95 Totalförsvarets fortsatta utveckling**

Propositionen från 86/87 ägnar mer utrymme åt telekommunikationer och diskuterar mer utförligt vilka åtgärder som bör vidtas än tidigare försvarspropositioner. Man rekommenderar dessutom en kraftig ökning av investeringsnivån. Motivet för detta är samhällets ökande beroende av telekommunikationer och den ökade medvetenheten om hot i form av sabotage vilket uppmärksammats i propositionens förarbeten.

Det civila totalförsvaret har funktionsindelats och det är Kommunikationsdepartementet som i propositionen redovisar inriktningen för funktionen Telekommunikationer. Det är dock fortfarande Televerkets uppgift att säkerställa att totalförsvarets alla delar har tillgång till telekommunikationer.

Televerket hade inför försvarsbeslutet, enligt regeringens anvisningar utarbetat en programplan avseende planerade beredskapsåtgärder i telenäten för perioden 1987/88-1991/92<sup>14</sup>. Programplanen hade som utgångspunkt att det behövdes en betydande höjning av ambitionsnivån i fråga om krigsskyddsåtgärder för telekommunikationssystemen. Utöver uthållighetshöjande åtgärder redovisar programplanen befintligt EMP-skydd, ADB-säkerhet i kriser och i krig, hot från sabotageförband mot televerket och skydd mot detta, samt hot från telekrigföring och motsvarande skyddsåtgärder.

I sitt slutbetänkande<sup>15</sup> konstaterar 1984 års försvarskommitté att samhällets kraftigt ökade behov av telekommunikationer bland annat beror på den snabba tekniska utvecklingen inom

<sup>12</sup> Ds Fö 1981:14 Totalförsvaret 1982/87

<sup>13</sup> I SSLPs RES-rapporter från 70-talet är komplexitet och koncentration uppmärksammade sårbarhetsfaktorer

<sup>14</sup> Programplan – Beredskapsåtgärder i televerkets nät 1987/77 – 1991/92, Televerket, juli 1986

<sup>15</sup> SOU 1987:9 Det svenska totalförsvaret inför 90-talet

ADB-området. Störningar som medför betydligt minskad kapacitet i telekommunikations-systemen kommer därför att få svåra följder för det civila samhället.

I mitten på 80-talet gjordes studier som uppmärksammade hot i form av sabotage<sup>16, 17</sup> vilket även påverkade försvarskommittén. Kommittén ansåg att strävan borde vara att telekommunikationer för totalförsvarsfunktioner med säkerhet måste kunna upprätthållas i godtagbar omfattning även under störda förhållanden. Detta borde enligt kommittén uppmärksammas i den fortsatta utbyggnaden av telenätet. Dessutom påpekade kommittén att man bör ägna telekommunikationerna i Norrland särskild uppmärksamhet. Kommittén kom till slutsatsen att det högsta av regeringen anvisade planeringsalternativen beträffande investeringar borde väljas.

I propositionen konstaterades att det finns ett nära samband mellan fredsmässiga krav på säkerhet och de som uppkommer i ett läge av beredskap och krig. Utifrån de argument som framfördes i propositionens förarbeten förordades således en avsevärd ambitionshöjning i investeringarna beträffande beredskapsåtgärder. Det framhölls även att Televerket skulle svara för finansiering av samtliga sina beredskapsåtgärder. Samtidigt skulle åtgärder som tillgodoser en enstaka totalförsvarsmyndighets behov finansieras av denna myndighet.

### **Central Säkerhetsplan (CS) för Televerkets säkerhetsverksamhet 1990 – 1992**

Försvarsbeslutet från 1987 är en av flera styrande faktorer för Televerkets säkerhetsplan från april 1989. Planen är indelad i sex områden: Samverkan, Beredskapsplanering, Utbildning, Krigsskydd, Marknad och Säkerhet. Inom varje område redogörs i planen för utgångslägen och mål för olika delar inom säkerhets- och beredskapsarbetet.

#### *Samverkan*

Avseende Samverkan så konstateras att behovet av detta är stort inom totalförsvarets telekommunikationsfunktion och att TTB (Totalförsvarets teleberedning) spelar en aktiv roll.

#### *Beredskapsplanläggning*

Beredskapsplanläggning innebär utfärdande av bestämmelser för Televerkets verksamhet och organisation, förberedande av planer samt säkerställande av krigsorganisationens personal- och materielförsörjning i kris och krig. De ytterligare åtgärder som föreslås inom detta område är mest revideringar och kompletteringar.

#### *Utbildning*

Inom området Utbildning genomförs säkerhetsutbildningar (ADB inkluderat), krigsbefattningsutbildningar, övningar och spel för ledningsfunktioner samt allmänt informationsarbete inom säkerhets- och försvarsberedskapsområdet.

#### *Krigsskydd*

Krigsskyddsåtgärder bekostades av Televerket. Ett antal allmänna mål nämns.

Exempelvis anges att hus och skalskydd för de mest betydelsefulla telesystemen skall förstärkas. En konkret åtgärd omfattar indelning av det digitala nätet i ett H-nät och ett V-nät, där H-nätets stationer skall placeras i berggrum och V-nätets stationer får skydd mot splitter och tryckvåg.

Transportabel reservutrustning för telefonstationerna i det analoga nätet rapporteras finnas i begränsad omfattning. Ett mål är därför en ökad satsning på anskaffning av transportabel utrustning. I planen nämns exempelvis transportabla radiolänkar, koncentratorer, AXE-stationer och utbrutna abonnentsteg.

<sup>16</sup> SKRIK-projektet vid FOA

<sup>17</sup> Sårbarhet och säkerhet i statlig ADB-verksamhet, konsekvenser och störningar, Statskontoret, 1986:3

För att uppnå mål om en hög grad av uthållighet skall man successivt trygga elkraftförsörjningen genom ytterligare reservverk och yttre anslutningsmöjligheter. I planen konstateras att stationära reservverk redan finns för alla större telefon-, förmedlings- och radiolänkstationer, samt att det för mindre stationer införskaffats transportabla reservverk.

Ett annat allmänt mål är att krigsviktiga kunder skall ges prioritet i krig, detta innebär bland annat att prioriterade abonnenter tilldelas tjänsten ”Prioritet” i de digitala AXE-växlarna som installeras.

#### *Marknad*

Detta är åtgärder för att tillgodose totalförsvarets kommunikationsbehov och som levereras av Televerket. Åtgärderna beställs och bekostas dock av andra myndigheter, organisationer och företag verksamma inom Totalförsvaret. Dessa åtgärder utgörs främst av speciell utrustning och speciella tjänster som exempelvis stela förbindelser<sup>18</sup>, Mx-utrustning<sup>19</sup>, alarmering, beredskapsväxlar och kvalificerad telesäkerhetsrådgivning.

#### *Säkerhet*

Åtgärder inom området säkerhet syftade till ökad säkerhet i fysisk och systemteknisk bemärkelse. Val av åtgärder grundades på hotstudier, riskanalys och riskinventering bekostade av Televerket själva. Detta område innehåller ett brett spektrum av åtgärder och har som mål att garantera försvarssäkerhet, egendomssäkerhet, personsäkerhet, ekonomisk säkerhet, kundsäkerhet, ADB-säkerhet, nätsäkerhet och systemsäkerhet. Exempel på åtgärder är personkontroll, tillträdesskydd, rutiner för hantering av dokument och kunduppgifter och ADB-säkerhetsrutiner.

### **2.3.3 1990-talet – Nya tider och marknadsreformer**

#### **Proposition 1990/91:102 om verksamhet och anslag inom totalförsvaret under budgetåret 1991/92**

I denna proposition anar man nya tider. Det säkerhetspolitiska läget är under förändring och Televerkets era närmar sig sitt slut. Ny teknik och de satsningar som beslutades om i 1986/87 år försvarsbeslut har gett resultat.

I propositionen konstaterades att många av de säkerhetsåtgärder som tidigare motiverades av krigshot nu införs av fredsmässiga driftsäkerhetsskäl, efterfrågade av säkerhetsmedvetna kunder. Detta har frigjort resurser för andra åtgärder, främst fullträffskydd för telestationer på högre nivå i näten. Fullträffskydd motiverades av att man i slutet av åttiotalet uppmärksammade hotet från precisionsvapen. De gamla skydden som skulle klara en så kallad ”närmis” dög inte längre.

Propositionen konstaterade att telekommunikationsbranschen är dynamisk och expansiv. Flera nya aktörer var på väg in på den allmänna marknaden. Det framhölls därför att televerkets ställning som funktionsansvarig myndighet behövde klarläggas.

#### **Proposition 1991/92:102 Totalförsvarets utveckling till och med budgetåret 1996/97 samt anslag för budgetåret 1992/93**

Propositionen förtydligar bland annat målen för funktionen Telekommunikationer genom att kvantifiera vissa tidskrav. Vid krigsutbrott skall totalförsvarsviktiga kunders teletrafik kunna ges prioritet inom ett dygn och deras teleanordningar skall kunna underhållas och repareras

<sup>18</sup> Stela förbindelser är en sätt att i det analoga nätet ordna förberedda förbindelser. Digitaliseringen av telenätet innebär att dessa försvann och ersattes av tjänster i det digitala nätet.

<sup>19</sup> Mx = Militärt exklusiv. Utrustning i Televerkets nät speciellt anpassad för snabb inkoppling av abonnemang mm.

omedelbart. Telekommunikationer för ledning och operativ verksamhet skall säkerställas så att angelägen trafik kan återupptas senast åtta timmar efter totalavbrott.

Televerket är 1992 fortfarande funktionsansvarig myndighet. Dock är det känt att televerket kommer att ombildas till aktiebolag den 1 juli 1993 och det konstateras i propositionen att Televerkets återstående myndighetsutövning då måste överföras till någon annan myndighet.

Televerkets programplan för 1992-1996<sup>20</sup> med komplettering<sup>21</sup> utgör en del av underlaget för propositionstexten. Denna programplan är inriktad mot en förstärkning av driftsäkerhet och krigsuthållighet vid televerkets anläggningar. I kompletteringen konstateras att den förändrade säkerhetspolitiska situationen inte föranleder verket att ompröva behovet av fortsatta beredskapsåtgärder. Däremot accentueras behovet av en ökad integration av dessa åtgärder för säkerhet i fred och katastrof. I programplanen påpekades istället att den snabba teknikutvecklingen kan leda till att föreslagna åtgärder och prioriteringar måste omprövas under perioden.<sup>22</sup>

### **Proposition 1996/97:4 Totalförsvaret i förnyelse – etapp 2**

En stor förändring i denna proposition är att målen för funktionen telekommunikationer nu får en inriktning mot fredstida hot. Enligt regeringens förslag skall verksamheten bedrivas så att totalförsvarets behov av teletjänster under höjd beredskap tillgodoses. Verksamheten skall även bedrivas så att de resurser och den beredskap som skapas också skall kunna utnyttjas vid svåra påfrestningar i fred.

Post och Telestyrelsen är nu funktionsansvarig myndighet för funktionen Telekommunikationer<sup>23</sup>. Det bedömda beredskapsläget baserar sig fortfarande i stor utsträckning på förhållandena i Telias nät. Dock konstateras att satsningen på en mångfald av operatörer ger ökad flexibilitet och minskad sårbarhet.

Sårbarheten anses vara stor för framförallt sabotage och precisionsstyrda vapen varför satsningar på skydd mot detta prioriteras. Detta innebär satsningar på redundans och omkopplingsmöjligheter samt spridning av vitala funktioner och förbättrat skydd av Telias transportnät. I propositionen sägs att manipulering av datasystem särskilt måste beaktas och att Post- och Telestyrelsen utreder hur åtgärder bör vidtas för att förhindra detta. Dessutom påpekas att GSM-systemen förbereds för användning i krig genom att vissa anläggningar fullträffskyddas. Man pekar också på behovet av att förbättra reservkraften för att klara långa elavbrott, liksom behovet av en metod för prioritering av totalförsvarsviktiga kunder.

För finansiering av teleberedskapen så föreslås ett avgiftssystem som omfattar vissa beredskapsåtgärder mot allvarliga fredstida hot och påfrestningar. Av de 200 miljoner som propositionen anger årligen erfordras för beredskapsåtgärder på teleområdet, skall hälften avgiftsfinansieras.

### **Proposition 1996/97:11 Beredskapen mot svåra påfrestningar på samhället i fred**

I 1992 års försvarsbeslut framhölls att det kunde finnas skäl att i särskild ordning överväga hur samhällets beredskap mot olika fredstida hot skulle stärkas. Detta resulterade i tillsättande av en parlamentarisk kommitté som valde att kalla sig Hot- och riskutredningen. Denna lämnade i januari 1995 sitt huvudbetänkande<sup>24</sup> samt en rad delbetänkanden<sup>25</sup> innehållande ett

<sup>20</sup> Programplan 1992-1996 funktionen Telekommunikationer, Televerket, augusti 1990

<sup>21</sup> Televerket, september 1991

<sup>22</sup> Det är alltså i detta fall den tekniska förändringen snarare än hotbilden som förändrar sårbarheten.

<sup>23</sup> Den 1 juli 1993 övertog Telestyrelsen Televerkets myndighetsansvar. I samband med Postens bolagisering 1994 övergick Telestyrelsen till att bli Post- och Telestyrelsen.

<sup>24</sup> SOU 1995:19 Ett säkrare samhälle

antal scenarion. Proposition 1996/97:11 tog ställning till vissa av de förslag som Hot- och riskutredningen lämnade beträffande åtgärder för att förbättra beredskapen mot svåra påfrestningar.

I propositionen konstaterades att telekommunikationerna har avgörande betydelse för samhällets funktionsförmåga och att det därför är väsentligt att sårbarheten mot fredstida hot byggs bort och begränsas. Man konstaterar att det allvarligaste fredstida hotet är sabotage samt att telekommunikationerna är känsliga för långvariga avbrott i elförsörjningen. De åtgärder som förordades är i stort desamma som i proposition 1996/97:4.

### **Skrivelse 1998/99:33 Beredskapen mot svåra påfrestningar på samhället i fred**

Enligt proposition 1996/97:11 skulle regeringen årligen lämna en redovisning avseende beredskapen mot svåra påfrestningar på samhället i fred.

Kommunikationsdepartementet konstaterar i skrivelsen att den starka kommersiella utvecklingen bidrar till en ökad tillgång på nya kommunikationsmöjligheter. Detta anses bidra till möjligheterna att öka telekommunikationernas robusthet om de positiva effekterna tillvaratas på ett framsynt sätt. Samtidigt ser man en risk i att detta kan ge nya sårbarheter. Vikten av kompetens hos PTS och teleoperatörer avseende förebyggande och hantering av svåra telestörningar betonas därför.

I propositionen redovisas beredskapsläget. De tekniska sårbarheter som pekas ut är dålig IT-säkerhet, koncentration av teknik, centralisering av nyckelfunktioner för styrning och övervakning, dåligt skyddade lokaler och otillräcklig reservkraft. Dessutom konstateras att det saknas möjlighet att prioritera samhällsviktiga abonnenter. Regeringen pekar också på en mängd hot mot telekommunikationerna IT-attacker, precisionsbekämpning med långräckviddiga luftburna vapen, störningar i elförsörjningen, naturkatastrofer, sabotage, terroristhandlingar samt HPM.

Dessutom listas de åtgärder som vidtagits av PTS under 1997. Dessa åtgärder omfattar bland annat färdigställande av sammankopplingspunkter mellan olika operatörers transmissionsnät, upphandling av mobila GSM-basstationer samt ett antal utredningar och övningar.

### **Proposition 1998/99:74 Förändrad omvärld – omdanat försvar**

I 1996 års försvarsbeslut beslutade riksdagen att säkerhetspolitiska kontrollstationer skulle genomföras under försvarsbeslutsperioden. Kontrollstationernas syften är att bidra till att det sker en fortlöpande politisk prövning av det säkerhetspolitiska läget och dess konsekvenser för totalförsvarets beredskap, omfattning, utveckling och förnyelse.

Regeringen anser i propositionen att samhällets beroende av fungerande telekommunikationer gör att funktionen kan vara en gränssättande faktor för hela totalförsvarets samlade förmåga. Regeringen anger även att samhällets tolerans för störningar i telekommunikationerna minskar.

Den hotbild som redovisas är densamma som i regeringens skrivelse 1998/99:33.

I propositionen bedöms telekommunikationerna kunna ha en godtagbar säkerhet för svåra störningar i fred och höjd beredskap inom några år. Denna bedömning anses dock vara osäker och regeringen vill att en genomgång av telefunktionen skall genomföras. Detta eftersom teknikutvecklingen är mycket snabb varför det sker snabba förändringar, såväl positiva som negativa, i telekommunikationernas sårbarhet.

---

<sup>25</sup> SOU 1995:20 Utan el stannar Sverige, SOU 1995:21 Staden på vattnet utan vatten, SOU 1995:22 Radioaktiva ämnen slår ut jordbruk i Skåne, SOU 1995:23 Brist på elektronikkomponenter, SOU 1995:24 Gasmoln lamslår Uppsala

Regeringen anser att PTS förslag till planeringsinriktning bestående av elva punkter som rimlig. Föreslagna åtgärder är bland annat åtgärder mot intrång i datanät, förstärkning av transmissionnät i områden där kommersiell drivkraft för detta saknas, identifiering och skydd av vitala delar av Internets funktionalitet, införande av prioritetssystem för samhällsviktiga funktioner, anskaffning av reservkraftsaggregat samt särskilda funktionsövningar med teleoperatörerna.

### 2.3.4 2000-talet – IT och konvergens

#### **Proposition 1999/2000:30 Det nya försvaret**

I denna proposition, där telekommunikationerna behandlas relativt kortfattat, konstateras att elförsörjningen är gränssättande för telekommunikationernas förmåga samt att de IT- och Internetrelaterade hoten mot telekommunikationerna blivit mer uppmärksammade.

Man konstaterar att beredskapen mot sådana störningar i telekommunikationerna som skulle kunna medföra svåra påfrestningar på samhället i fred har ett starkt samband med de beredskapsåtgärder som vidtas för krigstida störningar.

Det rapporteras även att PTS initierat intrångsanalyser hos teleoperatörerna samt att man beslutat ge ÖCB i uppdrag att genomföra en uppföljning av 1996 års funktionsgenomgång av funktionen Telekommunikationer.

#### **Skrivelse 2000/01:52 Beredskapen mot svåra påfrestningar på samhället i fred**

Denna skrivelse innehåller en omfattande bedömning av läget för beredskapen inom funktionen Telekommunikationer.

Regeringen konstaterar i skrivelsen att elförsörjningens beroende av tele- och radiokommunikationer är gränssättande (i proposition 1999/2000:30 konstaterades att även det omvända gäller), och att man avser att uppdraga åt Svenska Kraftnät att i samråd med PTS analysera de ömsesidiga beroendeförhållandena mellan el och tele vid långvariga och omfattande avbrott.

I skrivelsen konstateras att samhällets ökande beroende av väl fungerande kommunikationer minskar toleransen för avbrott och störningar. Regeringen gör bedömningen att telekommunikationernas beredskap inför svåra påfrestningar i fred kommer att vara godtagbar inom några år med bibehållna ekonomiska förutsättningar. Den tekniska utvecklingen med bland annat utbyggnad av optokabel och bredbandig mobil access anses kunna öka robustheten.

En rad hot och risker redovisas tillsammans med de åtgärder som PTS vidtagit för att minska sårbarheten. Regeringen gör sedan en bedömning av motståndsförmåga avseende vitala funktioner inom telekommunikationsområdet enligt följande:

Skydda av driftledning	Godtagbar
Elförsörjning	Ej godtagbar
Skydd mot IT-angrepp	Ej godtagbar
Internet, infrastruktur	Ej godtagbar
Prioritet av telefoni	Ej godtagbar
Hopkopplingspunkter mellan nät	Godtagbar
Transmission, nationell infrastruktur	Godtagbar

Bedömningen betecknas dock av regeringen som osäker eftersom utvecklingen inom området går mycket fort.

**Proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret**

Regeringen gör i propositionen bedömningen att telekommunikationerna är en nyckelfunktion inom totalförsvaret och att insatser för att förebygga att störningar inträffar bör ges fortsatt hög prioritet. Telekommunikationerna anses kunna vara ett av de första målen vid ett angrepp. Angrepp mot telekommunikationerna bedöms även kunna ske i fredstid i form av informationsoperationer, vilket gör att telekommunikationerna måste ha en god robusthet även i fredstid. Regeringen anger att vid ett väpnat angrepp skall målet vara att så långt som möjligt tillhandahålla de tjänster som finns i fred.

Regeringen pekar i propositionen på ett antal sårbarheter. Teknikutvecklingen och den kommersiella utvecklingen kan ge positiva effekter, men även leda till ökad centralisering och koncentring av nyckelfunktioner som styrning och övervakning. Det finns endast ett fåtal personer som har kompetens att hantera mer omfattande störningar. Telekommunikationerna är sårbara för långvariga avbrott i elförsörjningen. IT-intrång är ett potentiellt hot liksom HPM. Dessutom anger regeringen direkta fysiska hot i form av precisionsstyrda vapen och sabotageförband.

Regeringen anser att strategin för åtgärder bör vara att bygga bort sårbarheter i samband med nätutbyggnad och införande av ny teknik. Sårbarheter i transmissionsnät bör prioriteras. Sårbarheten för långa avbrott i elförsörjningen skall lösas med reservelförsörjning. Den utbyggnad av fullträffsskyddade teleanläggningar i berg som pågår bör slutföras. Dessutom upprepas att totalförsvarsviktiga abonnenter skall kunna ges prioritet avseende telefoni.

**Proposition 2001/02:158 Samhällets säkerhet och beredskap**

I propositionen konstateras att utvecklingen på telekommunikationsområdet karaktäriseras av fortsatt tillväxt av framför allt Internet och mobiltelefoni, konvergens mellan telefoni- och datatrafik, konvergens av mellan fast och mobil telefoni samt ökad utbyggnad av bandbredd i accessnätet.

Sårbarhets- och säkerhetsutredningens rapport<sup>26</sup> utgör en del av underlaget till propositionen. I denna framhålls samhällets ökade beroende av den tekniska infrastrukturen, samtidigt som olika infrastruktursystem blivit mer beroende av varandra. Samhället anses därmed ha blivit mer sårbart för störningar i den tekniska infrastrukturen. För teleområdet konstaterar utredningen att den tekniska utvecklingen är mycket snabb och att drivkrafterna bakom detta är kommersiella. Utredningen anser att detta medför en risk att sårbarhetsaspekterna nedprioriteras.

Även regeringens skrivelse Beredskapen mot svåra påfrestningar i fred<sup>27</sup> (se ovan) utgör ett viktigt underlag för propositionens text om beredskapen för telekommunikationerna, och regeringen står i propositionen fast vid sina bedömningar från denna skrivelse.

I propositionen redovisas utvecklingen inom några delar av telekommunikationsområdet som regeringen bedömer kommer att bidra till behovet av åtgärder. Konvergens mellan telekommunikationer, television, radio och IT (elektroniska kommunikationer) medför ett behov av regelförändringar. Utbyggnaden av IT-infrastruktur med hög överföringskapacitet medför att säkerhetsåtgärder vidtas i samband med utbyggnaden. Ett radiokommunikationssystem för samhällsviktiga användare kommer att behöva byggas. Tredje generationens mobiltelefoni är under utbyggnad och kräver eventuellt stöd i form av batteribackup.

<sup>26</sup> SOU 2001:41 Säkerhet i en ny tid

<sup>27</sup> Skrivelse 2000/01:52 Beredskapen mot svåra påfrestningar i fred



### 3 Elförsörjning

Med infrastruktur för elförsörjning avses såväl produktionsanläggningar för elkraft som överföringsnät och distributionsnät. I detta kapitel presenteras först kort och övergripande hur de tekniska systemen för elförsörjning har byggts upp och utvecklats. Därefter följer en beskrivning av hur sårbarheten har förändrats under de senaste 40 åren. Slutligen görs en genomgång av hur arbetet med dessa frågor har bedrivits på nationell nivå.

#### 3.1 System

El började användas för elektrisk belysning i Europa under 1870- och 1880-talen. Det var då fråga om likströmsanläggningar. Det var lokala företeelser med korta överföringsavstånd, det vill säga kraftproduktionen låg nära elkonsumtionen. På 1890-talet fick växelströmstekniken sitt genombrott och det blev möjligt att överföra elektrisk kraft på långa avstånd. Under 1900-talets första decennier byggdes regionala elsystem baserade på vattenkraft. Under 1920-talet började dessa regionala system att kopplas samman. Detta medförde driftsfördelar dels på grund av att antalet produktionskällor i ett nät ökade men även på grund av att fler abonnenter gav en jämnare last.

Sammankopplingen av regionala nät ledde under 1930-talet till en utveckling mot ett nationellt sammanhängande kraftsystem och före första världskriget var också det svenska kraftsystemet ett i teknisk mening enat system<sup>28</sup>. Stamnätet byggdes på 1930-talet med 220 kV ledningar. Under 1940-talet är det tydligt att elsystemet har en hierarki av nät med ett nationellt stamnät, regionnät och lokala distributionsnät. Under 1950-talet inleddes utbyggnaden av nuvarande 400 kV stamnät.

Efter andra världskriget påbörjades en kraftig utbyggnad av vattenkraften för att möta den stora ökningen av elkonsumtion. Elnäten förnyades och byggdes ut. Men man insåg att vattenkraftsresurserna var begränsade och man försökte därför hålla nere konsumtion som inte ansågs samhällsekonomiskt försvarbar<sup>29</sup>. På 60-talet sjönk oljepriserna vilket gjorde det lönsamt att även producera el med fossila bränslen en situation som förändrades med oljekrisen 1973. Försök med kärnkraft hade gjorts under 60-talet och 1972 startades Sveriges första kommersiella kärnkraftverk Oskarshamn 1. Utbyggnaden av kärnkraften fortsatte till 1985 då den tolfte och sista av Sveriges (idag elva) reaktorer togs i drift. Detta ledde bland annat till att svenska bostäder i stor utsträckning anpassades för uppvärmning med el istället för olja (se även Figur 1).

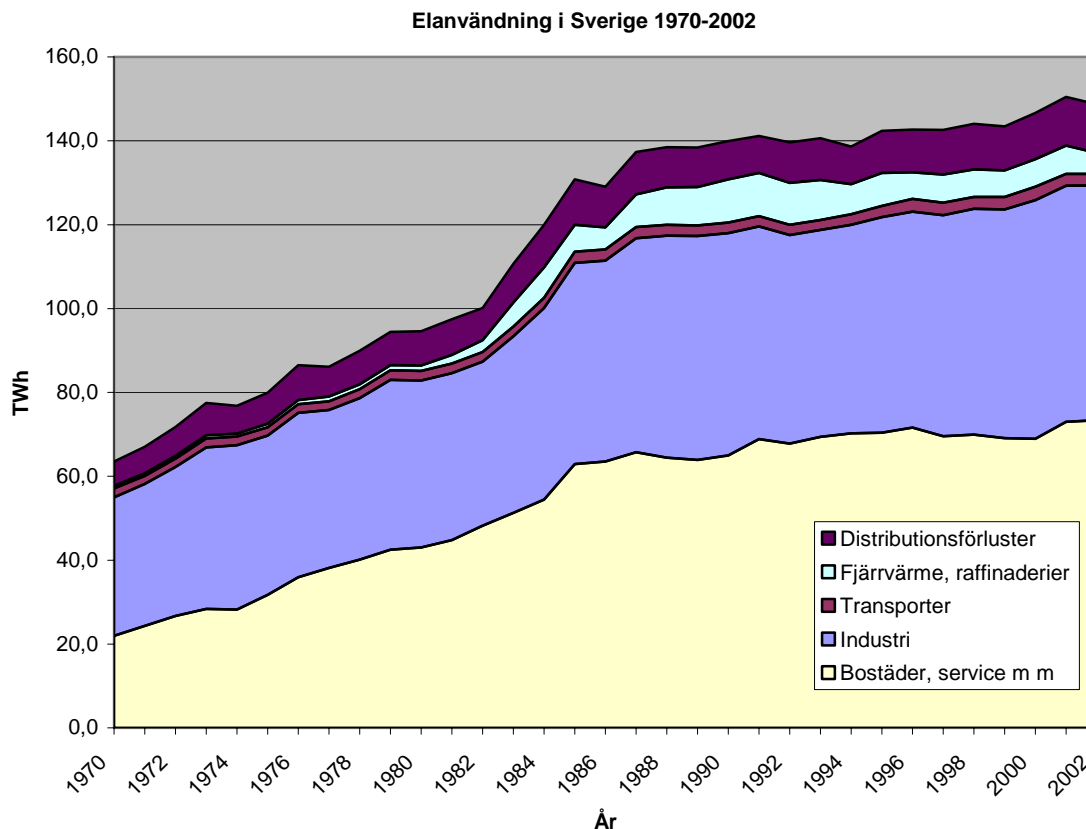
Under 1960-talet upprättades de första förbindelserna med våra nordiska grannländer. Under 1990-talet har det byggts likströmskablar till Polen och Tyskland. Det svenska elnätet har gått från att vara rent nationellt till att allt mer integreras i ett nordeuropeiskt elnät.

Mellan 1988 och 2002 har elanvändningen i Sverige ökat med endast i genomsnitt 0,5 % per år<sup>30</sup>. Det har därför inte funnits några behov av större nysatsningar på elförsörjningen. I början av 1990-talet då det dessutom började bli klart att elmarknaden skulle marknadsanpassas, minskade också nyinvesteringarna i produktions- och transmissionsanläggningar. På senare år har trenden snarare varit att produktionsanläggningar som inte varit ekonomiskt konkurrenskraftiga har avvecklats eller lagts i malpåse då det har varit billigare att effektivisera andra anläggningar eller importera el från utlandet.

<sup>28</sup> I fädrens spår, Arne Kaijser, 1994

<sup>29</sup> Vattenfall under 75 år, Statens Vattenfallsverk, 1984

<sup>30</sup> Energiläget 2003, Statens energimyndighet



**Figur 1** Fram till 1986 ökade elanvändningen kraftigt, framförallt var det bostäder, service m m som ökade sin elanvändning. Källa: Energiläget i siffror 2003, Statens energimyndighet

### 3.2 Sårbarheter

Ett stort problem för den svenska elförsörjningen är och har varit att en stor del av kraften produceras i norra Sverige medan konsumtionen huvudsakligen sker i söder. Det omfattande transmissionsnät som krävs för att överföra kraften utgör en stor sårbarhet. Den nya elproduktion som tillkommit, oljeeldad kraftvärme på 60-talet och kärnkraft på 70- och 80-talen har placerats i södra Sverige. Denna utbyggnad har dock inte tillkommit för att göra södra Sverige oberoende av norrländsk vattenkraft, utan har främst tjänat till att täcka ett ökande behov av elkraft i samhället.

En förändring ur sårbarhetssynpunkt är en ökande grad av automatisering. Detta är inte på något sätt unikt för elförsörjningen, utan påverkade all processindustri. Som påpekades i förra kapitlet är detta även en viktig faktor inom telekommunikationerna. Under 50- och 60-talen fanns det personal i varenda kraftstation. Införande av datorteknik och mer avancerade telesystem medförde möjligheten att upprätta driftcentraler som kunde styra och övervaka flera kraftstationer vilket effektiviserade driften, krävde mindre personal och således var mer ekonomiskt. En effekt av att personalen lämnar kraftstationerna är naturligtvis att stationerna inte har samma kontinuerliga övervakning som tidigare. En annan är att driftcentraler blivit känsliga punkter. Men central styrning och övervakning har även den fördelen att man snabbare kan reagera på och kompensera för eventuella störningar.

Personal som byggde näten var också den personal som fungerade som beredskapsorganisation i händelse av stora störningar. Minskningen i nyinvesteringar i början av 1990-talet ledde till att personalstyrkan och således även beredskapsorganisationen minskade.

Ett hot mot infrastrukturen för elförsörjning som uppmärksammats oftare på senare år är känsligheten för väder och vind. Det är häftiga snöfall och kraftiga vindar som får träd att falla över ledningar i lokalnäten som givit upphov till störningar. Uppmärksamheten har lett till ökade satsningar på isolerade ledningar och underhåll av ledningsgator.

När det gäller avsiktliga hot så är det den ökade precisionen vid angrepp genom luften som har lett till en ökad sårbarhet.

Vid sprängning av kärnvapen kan en, så kallad, elektromagnetisk puls ge skador på systemen för elförsörjning något som uppmärksammades under 1970-talet. Med det kalla krigets slut får dock risken för ett kärnvapenkrig i Europa anses ha minskat betydligt.

Den 27 december 1983 drabbades Sverige av ett stort elavbrott som satte fokus på elsystemets sårbarhet.

I mitten av 1980-talet uppmärksammades sabotage som ett allvarligt hot i beredskaps-sammanhang. Man konstaterade bland annat att elnäten var mycket sårbara för denna form av hot. Oron gällde framförallt angrepp mot stamnätet som skulle kunna ge nationella störningar. Man satsade därför på åtgärder för att möjliggöra ö-drift, vilket innebär att isolerad del av elnätet körs självförsörjande. Sabotagehotet ändrade karaktär under 1990-talet, från ett fokus på insatser av militära sabotageförband från främmande stater till att mer betraktas som ett möjligt tillvägagångssätt vid en terroristaktion.

Teknikutveckling i form av ökad automatisering har ju även medfört ett stort beroende av datorsystem. Precis som för telekommunikationerna öppnar detta upp för IT-hot i form av mjukvarubaserade attacker.

Den marknadsanpassning som elförsörjningen genomgått under 1990-talet har lett till avveckling av mindre lönsamma produktionsanläggningar. Till exempel så har det ansetts svårt att marknadsmässigt motivera gasturbiner, vilka behövs för en väl fungerande ö-drift.

Sedan 1960-talet har det svenska samhället blivit allt mer beroende av el. Detta beror till stor del på att våra bostäder anpassats för uppvärmning med el istället för med olja. Dessutom finns elberoende datorutrustning överallt och används dagligen. Tillförlitligheten i elförsörjningen medför också att beredskapen för längre elavbrott ofta är bristfällig såväl hos privatpersoner som inom företag. Kombinationen av ökat beroende och låg beredskap för avbrott medför att längre avbrott sannolikt får allvarligare konsekvenser idag än för 40 år sedan.

### **3.3 Nationella satsningar**

Inom elförsörjningen har det sedan 1930-talet vidtagits beredskapsåtgärder – så kallad elberedskap – med syfte att minska sårbarheten och öka driftsäkerheten i krig<sup>31</sup>. Åtgärderna har omfattat bland annat skydd mot sabotage och luftanfall (fortifikatoriskt skydd), förbättrad flexibilitet i överföringsnät och styrsystem, tillskapande av reservanläggningar och reparationsarbete.

#### **3.3.1 1970-talet och dessförinnan**

##### **SOU 1966:56 Svensk säkerhetspolitik – Förutsättningar och inriktning**

Denna utredning var avsedd att fungera som underlag för 1965 års försvarsutredning. Utredningen konstaterade att vattenkraften i huvudsak var den enda energikällan som var tillgänglig inom landet och att den bidrog till ca 40 % av energibehovet. De övriga 60 %

---

<sup>31</sup> Proposition 1998/99:74

tillgodosågs genom import av bränslen och drivmedel. En viktig åtgärd var därför att lagra bränslen. Det konstaterades även att elkraftnätets långa distributionslinjer från Norrland ner till mellersta och södra Sverige innebar en sårbarhet i krig. Tillkomsten av atomkraftverk kunde dock på längre sikt minska distributionsavstånden och därmed även sårbarheten.

### **Proposition 1976/77:74 om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling**

Statsmakterna har vid denna tidpunkt inte tagit ställning till någon målsättning för elkraftförsörjningen i olika kriser och krig. Istället är det Vattenfall som föreslår en målsättning för kraftförsörjningen under krig:

”Försörjningen med elektrisk energi skall under såväl fredskris som avspärning, krig och efterkris (krigs)tid tryggas för totalförsvarsfunktionerna och befolkningen i sådan omfattning att motståndsförmågan och samhällets viktigaste funktioner kan vidmakthållas.”

Propositionstexten baserar sig på den programplan<sup>32</sup> som Vattenfall tagit fram.

I programplanen rapporteras följande åtgärder ha vidtagits:

- studier rörande EMP-effekt på kraftsystem, bergförläggning av kärnkraftsanläggningar
- vissa förberedelser för konsumtionsreglering
- beredskapsplanläggning av kraftförsörjningen
- inventering av objekt för undanförelse och förstöring
- viss materialanskaffning
- beredskapslagring av olja
- utbildning och övning av kraftföretagens personal samt vapenfria tjänstepliktiga
- byggnadstekniskt skydd mot vapenverkan med innebörden att elkraftsanläggningar som är väsentliga för totalförsvaret, ges ett visst skydd efterhand de tillkommer.

I programplanen konstateras att det föreligger en viss brist på materiel på sambandssidan, vilket medför otillfredsställande sambandsvillkor för elkraftmyndigheterna.

Följande åtgärder avser man utföra under planeringsperioden 77/78-81/82

- medverkan i övergripande studier, utredningar och planeringsverksamhet
- förberedelser för konsumtionsreglering
- översyn av beredskapsverk och planer för elkraftsmyndigheter och företag
- anskaffning av reservutrustningar och övrig material
- beredskapslagring av olja, uran m m
- utbyggnad av elkraftmyndighetens samband
- utbildning och övning av krigsplacerad personal
- utbildning av vapenfria tjänstepliktiga
- byggnadstekniskt skydd

Kostnaderna beräknas för perioden uppgå till 130 miljoner kronor för Vattenfall och 125 miljoner kronor för övriga företag.

Programplanen konstaterar att den framtida energipolitiken i hög grad påverkar beredskapen inom elkraftsområdet.

<sup>32</sup> Programplan 1977/78 – 1981/82 för beredskapsverksamheten beträffande försörjningen med elkraft, Statens vattenfallsverk.

### 3.3.2 1980-talet – Sabotagehot och störning

#### Proposition 1981/82:102 om säkerhets- och försvarspolitiken samt totalförsvarets fortsatta utveckling

Målet för delprogrammet Elkraft föreslås i propositionen få inriktningen:

”Inom ramen för de allmänna målen för energiprogrammet bör målet för beredskapsverksamheten inom elkraftområdet vara att trygga samhällets behov av elenergi under fredskriser, avspärning och krig så att motståndsförmågan och de viktigaste funktionerna kan vidmakthållas.”

I övrigt anser propositionen att programplanen anger en lämplig inriktning.

I programplanen<sup>33</sup> rapporterar ÖEF att beredskapsorganisationen för krig är planlagd, personal och materielläge är tillfredställande och kräver endast smärre kompletteringar. Beredskapsorganisationen för en fredskris är under uppbyggnad men här återstår anvisning av planer och ytterligare utbildning av handläggare, däremot finns system förberedda för reglering av energiförbrukning.

ÖEF konstaterar att utvecklingen inom elvärmeområdet och utbyggnaden av kärnkraften är positiva ur beredskapssynpunkt då de leder till en minskad oljeförbrukning.

#### SOU 1984:69 Säker elförsörjning

Den 27 december 1983 drabbades den svenska elförsörjningen av en allvarlig störning som ledde till att kraftleveranserna avbröts till södra hälften av landet. Med anledning av den inträffade störningen beslutade regeringen 1984 att utreda elförsörjningens sårbarhet mot bakgrund av störningen och att lämna förslag till åtgärder för att minska sårbarheten i elförsörjningen och begränsa konsekvenserna av en omfattande störning. Utredningen lade fram ett antal överväganden och förslag beträffande elproduktion och stamnät inom följande områden:

- *Dimensioneringskriterier och riskbedömning.* Utredningen fann att arbetet inom detta område var ändamålsenligt och godtagbart.
- *Driftsäkerhet i stamnätet.* Här presenterades ett antal förslag på hur man genom nyanläggning, modernisering, utökad skyddsutrustning, reserver för spänningsstabilisering och mer utbildning och erfarenhetsåterföring skulle kunna öka driftsäkerheten i stamnätet.
- *Åtgärder i elproduktionsanläggningarna.* Man fann att det var angeläget med en översyn av utlösningsvillkor för kärnkraftsblocken vid nätstörningar, samt en översyn av kärn- och värmekraftsverkens förmåga till övergång till husturbindrift.
- *Från och tillkoppling av elbelastning.* Utredningen fann att erfarenheter från det decentraliserade systemet för driftåteruppbyggnad var goda.
- *Elförsörjning inom begränsade områden.* Utredningen fann att det inte var möjligt att klara en snabb övergång till drift på större separata system från ett spänningslöst läge, detta främst beroende på organisatoriska aspekter och reglertekniska svårigheter. Vid långa elavbrott fann man dock att det kunde finnas sådana möjligheter i några områden, något som ÖEF och Vattenfall skulle studera ytterligare.
- *Rollfördelning mellan berörda organisationer.* Utredningen fann att samarbetsformerna mellan Vattenfall och övriga kraftbolag var ändamålsenliga.

<sup>33</sup> Det ekonomiska försvarets programplan 1982/83-1986/87, ÖEF, 1981-08-27

### **Proposition 1986/87:95 Totalförsvarets fortsatta utveckling**

I en föredragning för 1984 års försvarskommitté<sup>34</sup> uppmärksammar Statens vattenfallsverk, som har ansvaret för delfunktionen Elkraft, att sabotageinsatser med relativt små medel kan ge betydande konsekvenser för samhället.

Vattenfall rapporterar att man inriktar den fredstida driften av stamnätet på att hålla nätet i en enhet. Dödnätstart av ett spänningslöst nät planeras starta från norr och sedan tas nätet successivt i drift söderut. Vattenfall konstaterar att den nya hotbilden (sabotageförband) kräver större flexibilitet vid driften av kraftsystemet. Vattenfall föreslår därför ö-drift, drift av större eller mindre kraftsystem skilda från övriga nätet, men påpekar att detta inte är förberett eller övat vare sig för fredsbruk eller för krig.

Dessutom rapporterar Vattenfall att de skadeförebyggande åtgärder som vidtagits inom drift, produktion och distribution samt de skadeavhjälpande resurser som kan organiseras är omfattande. Trots detta tror dock att en angripare sannolikt kan lamslå elförsörjningen under lång tid och man rekommenderar därför ökad anskaffning av reservkraftaggregat.

I propositionen påpekas att elförsörjningen är ett område som måste ges högsta prioritet i beredskapsplaneringen och att särskild uppmärksamhet bör ägnas åt distributionsnäten. Detta då betydelsen av en stabil eltillförsel är speciellt viktig för funktionssäkerheten hos transporter, telekommunikationer och kommunaltekniska system i samband med en krigsorganisering av samhället.

Propositionen föreslår att särskilda resurser avsätts för installationer av reservanordningar och åtgärder som möjliggör start och drift av separata delsystem<sup>35</sup>.

### **3.3.3 1990-talet – Organisatoriska förändringar**

#### **Proposition 1990/91:102 om verksamhet och anslag inom totalförsvaret under budgetåret 1991/92**

I propositionen föreslogs delfunktionen Elkraft få ett anslag på 32 miljoner kr för budgetåret 1991/92. Anslaget skulle betala kostnader för att stimulera andra kraftföretag än statens vattenfallsverk att vidta beredskapshöjande åtgärder i sin fredstida verksamhet. Det var fråga om bidrag till vissa tilläggsinvesteringar som kraft- och distributionsföretagen gjorde för att öka säkerheten i elsystemen, till exempel installation av reservanordningar och andra åtgärder som möjliggör start och drift av separata system.

Förslag<sup>36</sup> om omvandlingen av statens vattenfallsverk till aktiebolag den 1 januari 1992 noterades också i propositionen.

#### **Proposition 1991/92:102 Totalförsvarets utveckling till och med budgetåret 1996/97 samt anslag för budgetåret 1992/93**

I propositionen angavs målet för beredskapsverksamheten inom elkraftområdet vara att trygga samhällets behov av el under kriser och krig. Kraftföretagen, kommunerna och el-distributörerna skulle stimuleras till en ökad beredskapshänsyn i sin fredstida planering.

Statens vattenfallsverks ansvar för de myndighetsanknutna frågorna hade överförts till NUTEK, den branshanknutna operativa beredskapsplaneringen skulle hanteras av det av elbranschen organiserade och finansierade planeringskansliet Kraftsam. Affärsverket Svenska

<sup>34</sup> Elsystemets sårbarhet, B. Åqvist, Beredskapssektionen, Vattenfall, Föredragning PM för FK -84, 1984-12-19

<sup>35</sup> 1987 är det första året då Vattenfall får statliga medel för beredskapsåtgärder., tidigare har detta finansierats via egna medel. Vattenfall fick dock pengar för satsningar i andra kraftbolags anläggningar.

<sup>36</sup> Proposition 1990/91:87 om näringspolitik för tillväxt

kraftnät som från den 1 januari 1992 hade ansvaret för storkraftnätet svarade för beredskapsuppgiften på storkraftnätet.<sup>37</sup>

Propositionen påpekade att elförsörjningen är ett område som måste ges hög prioritet och NUTEK måste ges resurser för att stärka beredskapen bland annat genom installationer av reservanordningar, särskilda åtgärder i distributionsnäten och insatser som möjliggör start och drift av separata system.

### **Proposition 1996/97:4 Totalförsvaret i förnyelse – etapp 2**

Regeringens förslag till försvarsbeslut för 1997-2001 lades upp på ett nytt sätt. Den delades upp i två etapper, där den första etappen<sup>38</sup> innehöll mer principiella ställningstaganden. En sådan var att en helhetssyn skall präglade samhällets satsningar och åtgärder för att förebygga och hantera hot och risker i såväl fred som krig.

Delfunktionen Elkraft återfinns under funktionen Energiförsörjning. I propositionen föreslås målet för denna funktion vara att verksamheten skall bedrivas så att totalförsvarets och det övriga samhällets behov av elkraft under höjd beredskap kan tillgodose. De resurser och den beredskap som skapas skall även kunna utnyttjas vid svåra påfrestningar på samhället i fred.

I propositionen föreslås även att Affärsverket svenska kraftnät i fortsättningen skall vara ansvarig myndighet för delfunktionen Elförsörjning, samt att kostnaderna för åtgärder inom delfunktionen skall finansieras genom en elberedskapsavgift.

Avseende åtgärder så konstaterades att elförsörjningen liksom tidigare bör prioriteras. Verksamheten inom delfunktionen skulle inriktas mot:

- Fungerande elförsörjning för prioriterade användare
- Ytterligare utveckling och prövning av förutsättningarna för övergång till drift av elsystem i separata delsystem (ö-drift)
- Att reparationer för att upprätthålla och återupprätta ett sammanhängande elförsörjningssystem skall kunna genomföras
- Samordning av beredskapsåtgärder inom elförsörjning med de statliga insatserna för att installera reservkraftaggregat.

### **Proposition 1996/97:11 Beredskapen mot svåra påfrestningar på samhället i fred**

Proposition 1996/97:11 överlämnades till riksdagen samtidigt som proposition 1996/97:4 och ansågs av regeringen bilda en helhet.

I 1992 års försvarsbeslut framhölls att det kunde finnas skäl att i särskild ordning överväga hur samhällets beredskap mot olika fredstida hot skulle stärkas. Detta resulterade i tillsättande av en parlamentarisk kommitté som valde att kalla sig Hot- och riskutredningen. Denna lämnade i januari 1995 sitt huvudbetänkande<sup>39</sup> samt en rad delbetänkanden<sup>40</sup> innehållande ett antal scenarion. Proposition 1996/97:11 tar ställning till vissa av de förslag som Hot- och riskutredningen lämnade beträffande åtgärder för att förbättra beredskapen mot svåra påfrestningar.

<sup>37</sup> I praktiken flyttades Statens vattenfallsverks beredskapsenhet till Kraftsam och verksamheten kom att bedrivas av Svensk Elberedskap AB enligt avtal med NUTEK.

<sup>38</sup> Proposition 1995/96:12 Totalförsvaret i förnyelse

<sup>39</sup> SOU 1995:19 Ett säkrare samhälle

<sup>40</sup> SOU 1995:20 Utan el stannar Sverige, SOU 1995:21 Staden på vattnet utan vatten, SOU 1995:22 Radioaktiva ämnen slår ut jordbruk i Skåne, SOU 1995:23 Brist på elektronikkomponenter, SOU 1995:24 Gasmoln lamslår Uppsala

I propositionen konstaterades att elförsörjningen är av central betydelse för den ekonomiska och sociala utvecklingen i Sverige. Det var därför väsentligt att sårbarheten för fredstida störningar kunde begränsas och att känsligheten för störningar ytterligare reduceras. Propositionen föreslog att detta borde ske i samband med nätutbyggnad och införande av ny teknik inom elsystemet och hos förbrukare av el. Samtidigt konstaterade att kostnaderna för att helt eliminera elsystemens sårbarhet var mycket stora och att elförbrukarnas betalningsvilja borde vara vägledande för hur arbetet med att åstadkomma en god fredstida leveranssäkerhet skulle bedrivas.

Några av de åtgärder för att förstärka elförsörjningen som nämndes i proposition 1996/97:4 utvecklades ytterligare i proposition 1996/97:11.

#### *Prioriteringsordningar i samband med störningar i elförsörjningen*

Regeringen föreslog att det skulle tas fram planer för prioriteringar mellan funktioner i samhället i samband med störningar i elförsörjningen. Ett förslag till prioriteringsordning framtaget av ÖCB presenteras också.

#### *Prioritetsgrupp 1 (oundgängliga funktioner)*

- Ledningssystem (Civil ledning, geografiskt områdesansvariga myndigheter, viktigare funktionsledning, samverkan)
- Telekommunikationer
- Informations- och nyhetsförmedling samt radio- och TV-distribution
- Vitala verksamheter inom Försvarmakten
- Samhällsviktiga datasystem

#### *Prioritetsgrupp 2 (angelägna funktioner)*

- Polisväsende
- Hälso- och sjukvård m.m. (främst akutsjukvård och teknisk försörjning)
- Transporter (främst järnvägstransporter)
- Befolkningsskydd och räddningstjänst (främst förvarningssystem)
- Kommunalteknisk försörjning (främst dricksvatten- och värmeförsörjning)
- Livsmedelsförsörjning (främst varudistribution)
- Drivmedelsförsörjning (främst tankningsmöjligheter)
- Försörjning med industrivaror (främst reparationer av vitala funktioner och viss produktion för Försvarmaktens behov)

#### *Prioritetsgrupp 3 (övriga viktiga funktioner)*

- Socialförsäkring m.m.
- Postbefordran
- Finansiella tjänster
- Landskaps- och fastighetsinformation
- Övriga delar av vissa funktioner i prioritetsgrupperna 1 och 2 och som inte utpekats särskilt bör jämföras med funktioner i prioritetsgrupp 3.

Det konstaterades att ytterligare utredningsarbete krävdes och man föreslog att låta ÖCB genomföra detta.

#### *Ö-drift*

Regeringen föreslog att Svenska kraftnät skulle överväga förutsättningarna för ö-drift och vidta de åtgärder som erfordrades. Det konstaterades i propositionen att ö-driftsförfarande är komplicerat och att det aktualiseras först i samband med långvariga störningar.

#### *Reservkraftsaggregat*



För fredstida förhållanden ansåg regeringen att huvudprincipen borde vara att det är den enskilde som måste besluta om införskaffande av reservkraftaggregat utifrån ekonomiska bedömningar.

I propositionen påpekades att det statliga stöd som utgår för införskaffande av reservkraftaggregat för krigstida bruk bör fortsätta och i fortsättningen även grundas på behoven vid svåra påfrestningar på samhället i fred. Dessa insatser borde då samordnas med andra åtgärder för att trygga elförsörjningen i krig och vid svåra påfrestningar i fred.

Regeringen föreslog även att information om tillgången på reservkraftaggregat borde hållas samlad för länsstyrelsernas och andra myndigheters behov.

### **Proposition 1998/99:74 Förändrad omvärld – omdanat försvar**

I propositionen konstaterades att samhället blivit mer teknikberoende och därmed också mindre tolerant för störningar i elförsörjningen.

Några nya mål för inriktningen av beredskapsplaneringen redovisades inte i denna proposition. De som angavs i proposition 1996/97:4 låg kvar. Istället hänvisades till den övergripande strategi som NUTEK hade tagit fram i samråd med Svenska kraftnät och redovisat sommaren 1997.

Propositionen behandlade även Svenska kraftnäts verksamhetsplan för perioden 1997-2001. Enligt denna skulle åtgärder som ökar elförsörjningens uthållighet i ett långsiktigt perspektiv prioriteras framför åtgärder för kortsiktig handlingsberedskap. Idén var att elsystemet så långt som möjligt skulle drivas i en sammanhållen nationell drift. Om detta var omöjligt skulle försörjningen kunna ske i separata delsystem medan åtgärder vidtogs för återgång till nationellt sammanhållen drift. Mer konkret innebar denna strategi satsningar på

- fysiskt och tekniskt skydd av vitala anläggningar och driftledningscentraler
- åtgärder för ö-drift
- resurser för kraftsamlade reparationsinsatser på nationell och regional nivå.

Som mindre prioriterade alternativ utpekades åtgärder för mer kortsiktig handlingsberedskap såsom bränslelagring för elproduktion och anskaffning av vissa reservdelar.

Dessutom betonades åtgärder för ökad samverkan mellan de nordiska grannländerna, men även med övriga europeiska länder och i samband med internationella humanitära insatser.

Svenska kraftnät redovisade i sin verksamhetsplan även att åtgärder skulle vidtas för att stimulera företagen till en förbättrad störningsberedskap och att samordna denna beredskap.

Regeringen konstaterade även att elsystemet aldrig kan göras så säkert att en helt störningsfri elförsörjning kunde garanteras, varken i fred eller i krig. Verksamheter av stor betydelse för samhället måste därför vidta åtgärder för att minska beroendet av den ordinarie elförsörjningen. De åtgärder som förespråkades var fortsatt installation av reservkraft och ökad samordning av detta med de åtgärder som vidtas inom elsystemet. I propositionen refererades de riktlinjer som ÖCBs föreslagit för anskaffning och installation av reservkraftaggregat. ÖCB föreslog bland annat utredning av inrättande av reservkraftpooler. ÖCB föreslog även utredning av möjligheterna till omfördelning av reservkraftaggregat vid störningar.

### 3.3.4 2000-talet – Fokus på samhällets elberoende

#### **Regeringens skrivelse 2000/01:52 Beredskapen mot svåra påfrestningar på samhället i fred**

Näringsdepartementet redovisade elförsörjningens beredskap mot svåra påfrestningar i fred.

Det allvarligaste hotet i fredstid ansågs vara sabotage mot vitala delar av elsystemet. Regeringen konstaterade dock att elbortfall på landsbygden på grund av storm eller snöoväder är den vanligast förekommande störningen. Liksom i proposition 1998/99:74 konstaterades att samhällets elberoende ökar. Samhällsviktig verksamhet som skall fungera måste därför säkerställa sin tillgång till el även när den ordinarie elförsörjningen inte fungerar. De åtgärder regeringen ansåg borde genomföras var att:

- se till att en helhetssyn utvecklades som omfattade beredskapsåtgärder såväl på den el-operativa sidan som på användarsidan och att åtgärder skulle vägas emot varandra vad gäller kostnader och effekt,
- närmare analysera de ömsesidiga beroendena mellan el och tele,
- undersöka de tekniska möjligheterna att styra el till prioriterade användare,
- som en del av bevakningen av tillgång på reservkraft följa utvecklingen på gasturbinsidan i syfte att skapa bättre förutsättningar för drift av elsystemet i separata delsystem i en krissituation,
- studera möjligheterna att bergförlägga eller på annat sätt effektivt skydda strategisk, och svårreparerad utrustning i stam- och regionnät.

#### **SOU 2001:41 Säkerhet i en ny tid**

Sårbarhets- och säkerhetsutredningen konstaterade i sin rapport att när det gäller teknisk infrastruktur så intar elförsörjningen en särställning då flertalet samhällsverksamheter för sin funktion är beroende av en fungerande elförsörjning.

Utredningen föreslog en översyn av lagstiftningen i syfte att skärpa säkerhetskraven. Ett förslag var också förbättra tillsynen inom elområdet och ge säkerhetsaspekterna ett större utrymme. Genom att juridiska och tekniska åtgärder skulle det skapas möjligheter att prioritera samhällsviktiga användare vid störningar och avbrott i elförsörjningen. Utredningen konstaterade att reparationsresurserna framförallt gällande stam- och regionnäten är en gränssättande faktor för möjligheterna att upprätthålla elförsörjningen vid höjd beredskap, men även vid omfattande och oväntade skador i fred. Utredningen påpekade att utbildningsinsatser för att öka antalet montörer pågår, men föreslog även ändringar i elberedskapslagen för att kunna ställa högre krav på entreprenörföretag som utför underhåll på stam- och regionnät.

Utredningen ansåg också att en bättre samordning i planeringen av säkerhets- och beredskapsåtgärder mellan de myndigheter som är ansvariga för teknisk infrastruktur krävdes.

#### **Proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret**

Propositionstexten skiljde sig mycket lite mot vad som redovisades i Regeringens skrivelse 2000/01:52. Sårbarhets- och säkerhetsutredningens betänkande<sup>41</sup> omnämndes och det angavs att "Försvarsberedningen delar i allt väsentligt utredningens förslag"<sup>42</sup>.

<sup>41</sup> Säkerhet i en ny tid 2001:41

<sup>42</sup> Man får anta att regeringen med detta menar att försvarsberedningen delar Sårbarhets- och säkerhetsutredningens uppfattning om vilka förslag till åtgärder som är lämpliga.

**Proposition 2001/02:158 Samhällets säkerhet och beredskap**

Regeringen konstaterade i propositionen att Sverige under normala förhållanden har ett säkert elsystem, men att samhällets ökade elberoende och elsystemets känslighet för extrema väderförhållanden och organiserade våldsangrepp innebär att ytterligare åtgärder bör vidtas för att öka elsystemets uthållighet.

Regeringen gjorde i propositionen bedömningen att det finns ett tydligt samband mellan de beredskapsåtgärder som vidtas för situationer med höjd beredskap och åtgärdsbehovet för situationer med svåra störningar i fredstid.

Regeringen redovisade i propositionen några åtgärder som vidtas i stamnätet. För att öka överföringsförmågan studeras olika alternativ, bland annat att bygga om ställverk så att de blir mer robusta och att ombyggnader till 400 kV av befintliga ledningar för lägre spänningar.

Regeringen förordade en samordning av beredskaps- och skyddsåtgärder i anläggningar som förenat stam- och regionnät och noterar även att elbranschen tagit fram en praxis för informationsverksamhet i samband med större störningar. Elbranschen arbetade även med störstörningssamverkan och hade satt upp en målsättning som innebär att ingen nätkund skulle vara utan el i mer än 24 timmar. Flera elnätföretag hade avsatt extra medel för åtgärder inom områden med svagare eller mer utsatta nät. Svenska kraftnät rapporterade att man arbetade med kommunikations- och IT-säkerhet, undersökningar av tekniska möjligheter till att förbättra förmågan att prioritera användare och att med följa utvecklingen på gasturbin-sidan i syfte att skapa bättre förutsättningar för ö-drift. Svenska kraftnät arbetade även med att utbilda och organisera mobila reparationsenheter som bemannades av totalförsvarspliktiga.



## 4 Informationsförsörjning

Med informationsförsörjning avses den tekniska infrastrukturen i samhället som tillfredsställer samhällets behov av lagring och bearbetning av data. Det är de informationsbearbetande noderna och den funktion som dessa tillhandahåller som är det intressanta i denna presentation. Nät är inte i fokus vid behandlingen av detta område även om det kommer att beröras.

### 4.1 System

Sverige fick sin första dator i och med att BESK (Binär Elektronisk SekvensKalkylator) stod klar 1953. De första datorerna var utpräglade beräkningsmaskiner. Snart började man dock använda datorerna även för administrativ databehandling, bland annat registerföring och bearbetning av stora mängder data. I mitten på 60-talet börjar det dyka upp system i sådan omfattning och med sådan funktionalitet att det kan anses vara av betydande vikt för samhället, i huvudsak handlar det då om nationella befolkningsregister.

Datamaskinerna var vid denna tid mycket skrymmande, centralenheten fyllde hela rum. Inmatning kunde ske via tangentbord men vanligast var hålkort och hålremsor. Utmatning skedde till skrivare. Magnetband användes för lagring och återinläsning av data. Förutom att datorerna tog stor fysisk plats krävdes mycket personal för drift och programmering. Man hade även stansoperatriser som förberedde hålkort och hålremsor.

Direkt "on-line" kommunikation via teleförbindelser mellan datorer var möjlig men rekommenderades i början på 60-talet bara om det var oundgängligen nödvändigt med ögonblicklig behandling i datamaskinen<sup>43</sup>. Det ansågs vanligen bättre att låta kommunikation över teleförbindelser ske via de vanliga in- och utorganen (läsare och stansar för hålkort och hålremsor). Hålkort matades in i en läsare som läste av och via en teleförbindelse skickades data till en mottagande hålkortsstans som producerade nya hålkort. Vid lämpligt tillfälle matades dessa reproducerade hålkort in i datamaskinen.

Tio år senare i början på 70-talet har det skett en tydlig utveckling och den största mängden data sänds (on-line) via fast uppkopplad förbindelse<sup>44</sup>. Abonnenterna är dock flera i uppringd förbindelse än i fast uppkopplad. Fast uppkopplad förbindelse var mycket dyr och måste användas mycket för att ge lönsamhet.

Datorer hade blivit viktiga verktyg för registerföring och användes inom statsförvaltningen liksom av större banker och försäkringsbolag. Exempel på tillämpningar vid denna tid är befolkningsregister, körkortsregister och fastighetsregister. I en skrift från 1976, Datorerna och samhällets sårbarhet, konstaterades att "Den offentliga sektorn är idag i det närmaste fullständigt datoriserad."<sup>45</sup>

Under 70-talet blev datorerna fysiskt allt mindre. Samtidigt blev processorerna allt snabbare och minneskapaciteten för såväl primär- som sekundärminnen allt större. Dessutom utrustades datorerna med terminaler i form av bildskärmar och tangentbord vilket ökade tillgängligheten.

I slutet av 70-talet dök persondatorn upp, även om det stora genombrottet inte kom förrän under 1980-talet. En persondator är en egen fristående dator med egen processor, eget primärminne och lagringsenhet. Persondatorn i kombination med skrivbordsprogramvara som ordbehandlingsprogram, kalkylprogram och enklare databaser gjorde att kontoren datoriserades i allt större utsträckning. Skrivmaskinen konkurrerades ut och snart stod det en dator på varje skrivbord.

<sup>43</sup> SOU 1961:60 Den automatiska databehandlingens teknik

<sup>44</sup> Statskontorets rapport 1975:9, Data-skydd, Delrapport från statskontorets dataskyddsprojekt

<sup>45</sup> Datorerna och samhällets sårbarhet, s 34, 1976

Persondatorerna kopplades upp i lokala nätverk för att kunna dela på gemensamma resurser som skrivare och gemensamma hårddiskar. Persondatorerna kunde också fungera som terminaler mot olika stordatorregister. Skillnader i protokoll, hårdvara och mjukvara gjorde det dock relativt svårt att kommunicera mellan olika datorsystem. Det krävdes mycket anpassningsarbete och specialskrivna program för att konvertera data som utbyttes mellan olika system.

Utvecklingen av Internet Protocol, IP, påbörjades redan under 1960-talet som ett protokoll för kommunikation mellan datorer i nätverk och blev snart en allt mer allmänt använd standard. I slutet av 1980-talet etablerades Internet i Sverige Fördelen med ett standardiserat protokoll för kommunikation var att datorer från olika tillverkare och med olika operativsystem lätt kunde kommunicera med varandra. Användningen ökade explosivt under 1990-talet. Internet har gjort det lättare att såväl sprida som inhämta information. Det har även möjliggjort ett helt nytt sätt att kommunicera där text, bild och ljud alla kan användas. Framförallt e-post revolutionerade arbetet inom många områden.

Hela perioden karakteriseras av fullkomligt fantastiska prestandaförbättringar på alla plan. Systemen för informationsförsörjning har utvecklats från att vara isolerade stationer för lagring och bearbetning av data, till ett hopkopplat nätverk där även inhämtning, spridning och utbyte av information ingår som en naturlig del.

## **4.2 Sårbarheter**

I det följande är det *förändringen* i sårbarheter för systemen för informationsförsörjning som observeras och diskuteras.

Utvecklingen har gått från få och dyra stordatorer till miljontals relativt billiga servrar och skrivbordsdatorer uppkopplade i nätverk. Detta har fått en rad konsekvenser som påverkar sårbarheten. Stordatorn var en unik enhet som kunde ta lång tid att ersätta. Vilket innebar att varje dator hade stor betydelse för den verksamhet den skulle understödja. Idag är en enskild dator sällan kritisk på detta sätt.

Att datorerna var få och dyra innebar samtidigt att de helt naturligt omgärdades av en hög säkerhet. Det var värt att satsa pengar på tillträdesskydd, brandsäkerhet och reservkraft. Idag är detta inte alltid lika självklart då kostnaden för att skydda en enskild server kan överstiga kostnaden för servern många gånger om.

En avgörande faktor för ökad sårbarhet är de ökade kommunikationsmöjligheterna. Med Internet har systemen blivit allt mer tillgängliga på gott och ont. En bredare krets av användare ges möjlighet att utnyttja de tjänster som ett system kan erbjuda. Man kan därmed heller inte heller ha samma kontroll över vilka dessa användare är. Detta ställer höga krav på kontinuerligt uppdaterade säkerhetssystem.

Likaså har goda kommunikationsmöjligheter och öppna system möjliggjort överbelastningsattacker mot enskilda system. Genom att koordinera ett stort antal datorer att samtidigt initiera kommunikation med ett specifikt system hinner detta inte besvara alla förfrågningar och kan därigenom störas ut.

Utvecklingen mot standardisering av protokoll, operativsystem och programvaror har visserligen radikalt förbättrat möjligheten för integration och kommunikation mellan system. Samtidigt öppnar detta för att en standardprodukt med ett designfel som leder till en säkerhetslucka sprids till alla system som installerat produkten. Detta öppnar för att en attack som utnyttjar detta designfel kan massdupliceras och störa en stor mängd system samtidigt vilket kan ge upphov till kostsamma och svåra konsekvenser.

För datorsystem kan man argumentera att hot i form av fler mänskliga misstag och designfel har ökat. På 60- och 70-talen hanterades systemen av datorspecialister. Dessa var väl insatta i såväl hur både hårdvaran och mjukvaran fungerade. Vilket även innebar att de var medvetna om sårbarheter i systemen. Programmen var mindre och mer överblickbara vilket gjorde det lättare att få ett grepp om helheten. Komplexiteten i systemen har ökat kraftigt och det har blivit allt svårare att både besitta detaljkunskap, samtidigt som man har en översikt över ett system. Detta kan leda till felaktiga designbeslut som också påverkar säkerheten i systemen.

Datorerna har fått en bred spridning även bland användare som inte har någon speciell datorutbildning. Datorkunskapen bland dem som hanterar datorer är därför betydligt lägre med följderna att man inte är lika medveten om risker och problem. Möjligheten för misstag och slarv skulle ur denna synvinkel kunna sägas ha ökat. Samtidigt är systemen idag i högre grad designade för att vara användbara även av dem som inte är experter.

Om man ser på nya antagonistiska hot så är det möjligen elektromagnetiska vapen som har tillkommit. Risk för elektromagnetiska pulser från kärnvapen (EMP) har funnits länge men uppmärksammades med början på 70-talet. HPM-vapen<sup>46</sup> för mer riktade attacker med har diskuterats som ett hot under 90-talet.

IT-vapen<sup>47</sup> är ett hot som har utvecklats i samma takt som informationssystemen själva. Ny teknik ger nya möjligheter, möjligheter även för utveckling av nya vapen. På 1980-talet spreds exempelvis virus via disketter. Med Internet kom e-post och en helt ny kanal för spridning av virus. Internet har gjort det möjligt för en angripare att nå nästan vilka mål som helst, därmed inte sagt att angriparen har möjlighet att uppnå önskad verkan i målet. Standardisering av programvara medför även att ett och samma vapen kan användas mot ett stort antal mål.

Akvedukter och kloaker i det gamla Romarriket möjliggjorde större och mer avancerade städer samtidigt som det innebar att man var tvungen att förlita sig på att denna infrastruktur skulle fungera. På samma sätt är det med informationsteknologin idag. Den genomsyrar hela det moderna samhället och vi blir mer och mer beroende av att systemen skall fungera utan störningar. Längre fanns det manuella rutiner och tillräckligt med personal med rätt kompetens att ta till för den händelse att systemen inte skulle fungera. Men allteftersom datavolymerna har blivit allt större och tekniken mer avancerad och tillförlitlig har denna kapacitet utvecklats. Alternativa rutiner är inte längre ett alternativ.

### **4.3 Nationella satsningar**

Hantering av säkerhets- och beredskapsfrågor när det gäller infrastrukturen för informationsförsörjning är inte lika tydlig som för elförsörjningen och telekommunikationerna. För el och tele har dessa frågor alltid haft en organisatorisk hemvist hos någon eller några myndigheter. När det gäller informationsförsörjning har detta ansvar varit utspritt och fördelat på de verksamheter inklusive myndigheter som använder sig av olika datorsystem.

På nationell nivå genomförs satsningar vanligen i form av utredningar och sedan utfärdas riktlinjer och rekommendationer som varje verksamhet tolkar och följer på det sätt som passar just deras omständigheter.

<sup>46</sup> HPM – High Power Microwave

<sup>47</sup> IT-vapen är datorprogram vars funktion är att ge brukaren övertag gentemot en annan part genom att angripa datorsystem. Definition ur TEBIT – Teknisk beskrivningsmodell för IT-vapen, FOI-R--0305--SE, augusti 2002

”Frågan spänner över hela samhället, den följer inga departementsgränser, och det gör att olika beslutsfattare har svårt att se och känna ansvar för helheten.”<sup>48</sup>

I detta arbete blir redogörelsen för vilka nationella satsningar som genomförts därför fokuserad på initiativ i form av utredningar och rekommendationer. Det finns inget anspråk på att vara heltäckande utan de initiativ, utredningar och arbeten som behandlas är valda för att representera utvecklingen inom området under tidsperioden från slutet av 60-talet och framåt. Förhoppningen är att därigenom kunna visa på hur frågor runt säkerhet i informationsförsörjningen har behandlats vid olika tidpunkter.

### 4.3.1 1970-talet – ADB-säkerhet, en ny fråga

#### **ADB vid beredskap, Industrins försvarsbyrå, 1972**

Denna broschyr utgiven av Industrins försvarsbyrå vid Svenska arbetsgivarförbundet i syfte att främja och underlätta datorinnehavares beredskapsplanläggning. De föreslagna åtgärderna togs ursprungligen fram av en av ÖEF tillsatt arbetsgrupp (Data under beredskap och krig – DBK 71). Det konstaterades att vissa åtgärder också tjänar den framtida verksamheten. De åtgärder som föreslogs var:

##### *Prioritering av ADB-resurser*

I ett krisläge avsåg ÖEF att inhämta uppgifter om befintlig datakapacitet samt angelägenhetsgradera behovet av ADB, detta för att kunna genomföra prioriteringar om detta visade sig nödvändigt.

##### *Undanförsel*

Att flytta hela datorer sågs som en mycket kostsam åtgärd, förenad med stora olägenheter och skulle därför tillgripas endast i undantagsfall. Däremot rekommenderade ÖEF planläggning för undanförsel av reservdelar och tillbehör.

##### *Hänvisning till annan datacentral*

Detta innebar flytt av ett företags databehandling till en alternativ datacentral. Denna möjlighet ansågs dock begränsad.

##### *Personal*

ADB-personalen, främst driftpersonal och programmerare, var att betrakta som nyckelpersonal vilket man skulle ta hänsyn till i planeringen. Om personalbrist uppstod vid beredskap kunde värnpliktiga med särskilt kvalificerade uppgifter vid K-företag beviljas uppskov.

##### *Elkraft*

En möjlig åtgärd som nämns är installation av ett komplett ”no-break-system”, det vill säga batterier och reservaggregat.

##### *Teleförbindelser*

Det var televerket – i samarbete med länsstyrelserna – som planerade för att prioritera och säkerställa teleförbindelserna för totalförsvarsviktiga organ, genom att exempelvis ge förtur vid reparation. Televerket hade vid denna tid ingen speciell beredskapsplanläggning för teleförbindelser för dataöverföring.

##### *Service och reservdelar*

Datamaskinleverantörerna svarade som regel för all service och reparation och deras serviceavdelningar var därför beredskapsplanlagda. Datorleverantörernas lager av reservdelar

<sup>48</sup> Citat av Allan Erikssons avsnitt Sårbara datorer i SSLP en skrift tillägnad Lennart Grape, 1981



förutsågs räcka i 4-6 månader, med reservation för vissa delar som inte lagerhölls över huvud taget. En möjlighet för att tillgodose reservdelsbehovet vid krig bedömdes vara att "slakta" de datorer som inte användes i krig.

#### *Datatillbehör*

Med datatillbehör avsågs databärare (magnetband o dyl) och förbrukningsmaterial (hålkort, hålremsor etc). För denna typ av material fanns förberedd krigsproduktion.

#### *Transporter*

Man räknade med att en ökad andel dataöverföring i krig skulle ske med transporter såsom bil, järnväg och flyg. Dessa behov skulle uppmärksammas i krigstransportplanläggningen.

#### *Utlivningsberedskap*

Vid ett skärpt krisläge ansågs att det kunde vara lämpligt att skriva ut listor och sammanställningar av viktig lagrad information. Detta för att man skulle kunna övergå till manuella rutiner. Vad som skulle skrivas ut och hur detta skulle ske borde planeras redan i fred.

#### *Sekretess och säkerhet*

Detta kunde exempelvis innebära förstärkt tillträdesskydd och bevakning, tekniska skydd som lås och larm, förvaring av kopior av programbibliotek och data på säkra ställen, säkra transporter av sekretesskyddad information och förstöring.

#### *Katastrofskydd*

Detta kunde innebära ytterligare åtgärder avseende instruktioner för personalen vid katastroftillbud, övningar, skydd mot brand och vattenskador samt nödbelysning.

De två sist nämnda åtgärderna ansåg ÖEF inte vara någon speciell verksamhet för att tillgodose beredskapskrav, utan snarare åtgärder som många av datorinnehavarna redan vidtog.

### **SSLP och samhällets sårbarhet**

På försvarsdepartementet skapades 1972 Sekretariatet för säkerhetspolitik och långsiktplanering inom totalförsvaret (SSLP). Syftet med SSLP var att leda de studier och sammanställa det underlag som det nya planeringssystemet<sup>49</sup> krävde för att inrikta de olika totalförsvargrenarna. Inom SSLP formades tre referensgrupper varav en studerade svensk samhällsutveckling (RES – Referensgruppen för svensk samhällsutveckling). RES diskuterade utvecklingstendenser inom olika samhällssektorer i syfte att belysa de sårbara punkterna. En tydlig tendens var att verksamheten inom de olika sektorerna snabbt höll på att datoriseras. En speciell arbetsgrupp fick därför i uppdrag att studera detta och lade 1976 fram sin rapport "Datorerna". Denna rapport blev uppmärksammas och ledde i sin tur till att sårbarhetskommittén (SÅRK) tillsatts.

I rapporten gjordes en bedömning av hur teknik för data- och informationsbehandling kommer att utvecklas. Rapporten gjorde även prognoser inom ett antal tillämpningsområden:

- Industriella tillämpningar, övervakning, kontroll och styrning
- Planering, företagsledning och administration
- Databassystem
- Dokumenthantering och ekonomiska transaktioner
- Sjukvård
- Offentliga dataregister

<sup>49</sup> Ett förslag till nytt planeringssystem för totalförsvaret presenterades 1969 i utredningen Planering och programbudgetering inom försvaret (SOU 1969:25). Systemet godkändes av riksdagen 1970.

Därefter diskuterades sårbarheter, dels dator- och datasäkerhet men även samhällets sårbarhet. Rapporten konstaterade att införandet av datorer innebar en irreversibel process och leder till ökad sårbarhet inom ett antal områden. Bland annat pekade rapporten ut verksamheter som tidigare dominerats av arbetsintensiv produktionsteknik eller hantering av stora datamängder (exempelvis olika former av ekonomiska transaktioner) och att många verksamheter fick ett ökat beroende av realtidsbearbetning och datorkommunikation. Slutsatsen var att på sikt måste en minskning av sårbarheten basera sig på tekniska lösningar och inte på förhoppningar om att kunna återgå till manuella rutiner.

Rapporten drog även ett antal slutsatser av betydelse från totalförvarssynpunkt:

- Det krävs åtgärder för att minska risken att viktiga befolkningsregister faller i orätta händer
- Stora mängder information koncentreras till ett fåtal datacentraler och servicebyråer.
- I en krigssituation torde det vara realistiskt att förutsätta att ADB-tekniken endast kan utnyttjas i mycket begränsad omfattning då man är helt beroende av import.
- Av tillgänglig datorkapacitet är 80 procent koncentrerat till Storstockholmsområdet.
- Datakommunikationen över gränserna utvecklas snabbt och information bearbetas utomlands.
- Den ökade datoriseringen kommer att kräva en säkerhetsberedskap av helt ny omfattning och helt annat innehåll än tidigare.

### **Sårbarhetskommittén, SÅRK**

Sårbarhetskommittén (SÅRK) tillsattes enligt beslut av regeringen den 26 maj 1977. Uppgiften var att utreda sårbarheten hos det datoriserade samhället och föreslå åtgärder för att minska denna. SÅRK lämnade en lägesrapport i juni 1978<sup>50</sup> och sin slutrapport i december 1979<sup>51</sup>. SÅRK identifierade en mängd olika sårbarhetsfaktorer och kategoriserade dessa som yttre och inre sårbarhetsfaktorer<sup>52</sup>. De sårbarhetsfaktorer som identifierades var översiktligt:

#### *Yttre sårbarhetsfaktorer*

- Kriminella handlingar såsom sabotage, spioneri, förmögenhetsbrott och terrorism.
- Missbruk för politiska syften exempelvis blockad mot import av reservdelar, avstängning av kommunikationsledningar som passerar andra länder och infiltration.
- Krigshandlingar
- Katastrofer och olyckshändelser

#### *Inre sårbarhetsfaktorer*

- Innehållsmässigt känsliga register med detta avsågs närmast faran av att obehöriga för tillgång till eller missbrukar känslig information som lagras i systemen.
- Funktionellt känsliga system
- Koncentration. Här talade man om geografisk och funktionell koncentration. Med geografisk koncentration avsågs stor ansamling av datorkraft till vissa områden. Med funktionell koncentration avsågs stora centrala system med central drift och många kunder.

<sup>50</sup> Ds Fö 1978:4 ADB och samhällets sårbarhet

<sup>51</sup> SOU 1979:93 ADB och samhällets sårbarhet överväganden och förslag

<sup>52</sup> Yttre sårbarhetsfaktorer är närmast att klassificera som yttre hot och inre sårbarhetsfaktorer en blandning av datorsystemens egenskaper, användningsområden, svagheter och brister. SÅRK var själva inte helt nöjda med sin indelning utan konstaterade att "SÅRKs uppdelning av sårbarhetsfaktorerna kan inte strikt upprätthållas och ter sig därför möjligen diskutabel", sidan 33.

- Integration och inbördes beroende. Det faktum att datorsystem är beroende av varandra.
- Bearbetningsmöjligheter vid ansamling av stora datamängder. Med detta avsågs huvudsakligen att existerade register kan användas för att vaska fram ny känslig information.
- Bristfällig utbildning framförallt gällde detta datoranvändarnas kunskap om säkerhets- och sårbarhetsfrågor.
- Bristande kvalitet i fråga om maskin- och programvara
- Nyckelpersoner för datordriften
- Dokumentation det vill säga brister i dokumentation av systemen.
- Katastrofberedskap det vill säga avsaknad av planering för katastrofer.
- Utlandsberoende avseende komponenter, service, programvara och behörighetssystem.
- Datakommunikationsteknik
- Möjligheten att sprida datorkraft
- Standardisering av maskin- och programvara

SÅRK redogjorde även för vissa departements och myndigheters ansvar för ADB.

SÅRKs slutsats var att sårbarheten i samhället var oacceptabelt hög. Främst ansågs sårbarhet föreligga beträffande de stora centrala systemen och datoranläggningarna. Enligt SÅRK var orsakerna till detta främst att statsmakerna inte styr utvecklingen. De skulle tidigare ha kartlagt konsekvensen av samhällets datorisering och meddelat riktlinjerna för detta.

SÅRKs förslag till åtgärder för att motverka sårbarheten var att:

- Tillståndspröva datoranvändning
  - inom hela den offentliga sektorn (försvarsmakten undantagen),
  - inom den del av den privata sektorn som för ADB-baserade befolkningsregister.
- Inrätta Datainspektionen som tillstånds- och tillsynsmyndighet med möjlighet att ge föreskrifter.
- Införa anmälningsplikt för datoranvändande företag och organisationer till ÖEF.
- Ge aktiv information och rådgivning till datoranvändande företag och organisationer.
- Inrätta ett rådgivande organ till Datainspektionen gällande sårbarhetsfrågor.

I remissyttranden till SÅRK:s förslag<sup>53</sup> instämde ett flertal av remissinstanserna i SÅRK:s bedömning att sårbarheten var oacceptabel och att motåtgärder behövdes. Däremot var många negativa till att införa tillstånds- och anmälningsförfarande som man beförde skulle leda till en ökad byråkratisering. Istället efterlystes mer reella skyddsfunktioner och ett ställnings-tagande till vad som kan anses utgöra en acceptabel sårbarhet. Många remissinstanser menade att ökad medvetenhet genom information och rådgivning var den främsta metoden att uppnå minskad sårbarhet.

#### 4.3.2 1980-talet – Tekniken mognar

##### Sårbarhetsberedningen, SÅRB

Istället för att införa den lagstiftning som SÅRK föreslagit ville regeringen genom information och rådgivning öka datoranvändarnas medvetande om problemen och inspirera

<sup>53</sup> Uppgifterna om remissyttranden över SÅRK:s betänkande är hämtade från SÅRB:s slutrapport SOU 1986:12 Datorer sårbarhet säkerhet.

dem till åtgärder på frivillig väg. Regeringen beslöt därför i juli 1981 att tillsätta sårbarhetsberedningen, SÅRB. SÅRB skulle vara ett aktivt organ för information och rådgivning om sårbarhetsfrågorna i anknytning till ADB-verksamheten. SÅRB fick i uppgift att

- utarbeta en handlingsplan,
- vara ett rådgivande organ,
- pröva vilka åtgärder som kan behöva vidtas för att få till stånd en allmän information och rådgivning i frågor rörande säkerhet och sårbarhet i samband med utveckling och användning av ADB-system i samhället,
- tills vidare svara för information och rådgivning till både den offentliga och den privata sektorn,
- fungera som remissinstans på sårbarhetsområdet, främst vid investeringar i stora statliga datasystem,
- göra en fortsatt och fördjupad analys av sårbarheten och bedöma behovet av åtgärder,
- lägga grunden till en fortlöpande bevakning av sårbarhetsfrågorna och ta fram underlag till mera permanenta åtgärder.

SÅRBs mandat var tidsbegränsat till juli 1984 men förlängdes genom tilläggsdirektiv till utgången av 1985. I januari 1986 lade SÅRB fram sin slutrapport SOU 1986:12 Datorer säkerhet sårbarhet. SÅRB sökte ett brett samarbete med näringslivet, framträdde flitigt på konferenser och seminarier och hade täta och goda relationer med massmedia. Man bedrev flera av sina projekt i nära samarbete med icke-statliga organ. Några av projekten presenteras nedan.

#### *Metod för sårbarhetsprövning - SBA-metoden*

SÅRB ansåg att det krävdes ett strukturerat och metodiskt angreppssätt på sårbarhetsfrågorna och man beslutade att ta fram metoder och rutiner för sårbarhetsprövning av ADB-system. I början av 1992 började man därför utvecklingen av SBA-metoden i samarbete med Riksdataförbundet. SBA-metoden finns fortfarande (2003) och förvaltas numera av Dataföreningen i Sverige<sup>54</sup>. Metoden innebär en stark tilltro till kunskaper hos personal och individer i den analyserade verksamheten eller organisationen. Ansatsen bygger på att det är de som praktiskt arbetar med de vardagsnära problemen, oavsett hierarkisk nivå, som har störst möjlighet att lyfta fram de viktigaste problemen och ge förslag på lösningar.

#### *Utlandsberoendet*

Denna fråga utreddes redan av SÅRK men då beroendet av utlandet ansågs ha ökat ytterligare gick SÅRB vidare med frågan och gjorde ytterligare analyser av utlandsberoendet som en sårbarhetsfaktor.

#### *Utslagen datorkapacitet*

Projektet syftade till att mera generellt och principiellt beskriva vilka olika alternativ som finns vid utslagen datorkapacitet, för- och nackdelar med de olika alternativen och vad som kan påverka valet av dem.

#### *Personalrelaterade faktorer*

I ett par projekt behandlade SÅRB frågor om beroende av nyckelpersoner och frågor om rekrytering, utbildning arbetsmiljö och organisation av ADB-verksamhet, beredningen ansåg dock att det fanns mer att utreda och behandla inom området.

---

<sup>54</sup> Dataföreningen i Sverige bildades 1990 genom fusion av de tre organisationerna Riksdataförbundet, Svenska Dataföreningen och Svenska Samfundet för Informationsbehandling.

*ADB-systemens komplexitet*

SÅRB oroades av att systemen blev allt mer komplexa och svåra att överblicka. ”Självklart kan man inte skydda ett system om man inte kontrollerar det och känner dess gränser”, ansåg SÅRB. Lösningen var att förändra systemutvecklingsmetodiken samt att satsa på forskning om systemkomplexitet och datakvalitet.

*Datakommunikation*

SÅRB konstaterade att datakommunikationen hade ökat i omfattning vilket gett upphov till en ökad sårbarhet.

**Samrådsgruppen för samhällets säkerhet inom dataområdet, SAMS**

Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS) – en arbetsgrupp på Civildepartementet (1986-1991) och därefter på Finansdepartementet (1991-1993) – arbetade med frågor avseende ADB och samhällets säkerhet på 1990-talet.

Samrådsgruppens uppgift var att analysera samhällsviktiga säkerhetsfrågor inom dataområdet och lägga fram förslag för att öka säkerheten och minska sårbarheten. SAMS skulle dessutom genomföra analyser av datasäkerheten i samhällssektorer och i enskilda informationssystem, stödja departementen i datasäkerhetsfrågor, förbereda för Sveriges medverkan i EG:s arbete angående informationssystemens säkerhet, pröva om samhället har en effektiv organisation för säkerhetsarbetet samt stödja datasäkerhetsarbetet i samhället. SAMS lade våren 1990 fram fem rapporter (Ds 1990:43-47)

- De verksamhetsansvarigas säkerhetsansvar, Ds 1990:43
- Samhällsaspekter på säkerheten inom betalningsväsendet, Ds 1990:44
- Datakriminalitet i Sverige, Ds 1990:45
- Strukturfrågor och säkerhet, Ds 1990:46 och
- Datakommunikation och säkerhet, Ds 1990:47.

I rapporten ”De verksamhetsansvarigas säkerhetsansvar” (Ds 1990:43) konstaterades bland annat att det behövdes en översyn av revisionens roll och förutsättningar när det gällde uppföljning och kontroll av säkerheten i organisationers allt mer datorbaserade verksamheter. SAMS föreslog fler granskningar liknande den som SAMS själva genomfört rörande betalningsväsendet (Ds 1990:44). Myndigheter utanför statsförvaltningen, organisationer och företag borde genomföra säkerhetsanalyser för att klarlägga säkerhetsnivån hos väsentliga ADB-system och ta fram handlingsplaner för säkerhetsåtgärder. SAMS konstaterade också att flera statliga organ som Statskontoret, ÖCB, Överbefälhavaren och Rikspolisstyrelsen alla arbetade med att ta fram riktlinjer och handböcker rörande datasäkerhet. SAMS ansåg att detta arbete borde kunna utnyttjas för att skapa ett vidgat samarbete på samhällsnivå inom IT-säkerhetsområdet.

SAMS studerade den decentralisering av datorsystemens struktur som påbörjats under 80-talet och diskuterade detta ur säkerhetssynpunkt i rapporten ”Strukturfrågor och säkerhet” (Ds 1990:46). SAMS konstaterade dock att det inte finns något generellt samband mellan struktur och säkerhet, utan val av systemstruktur får olika konsekvenser för säkerheten och dessa måste beaktas. SAMS uppmärksammade även det ökande användandet av datakommunikation i sin rapport ”Datakommunikation och säkerhet” (Ds 1990:47). Slutsatsen var att säkerhetsmedvetandet hos användarna var bristfälligt och att användandet av datakommunikation borde säkerhetsanalyseras oftare än vad som var fallet.

I sin slutrapport från 1993 ansåg SAMS att det behövdes en kvalificerad funktion av det slag SAMS varit, för att hantera information om erfarenheter och problem runt informations-säkerhetsfrågor. I rapporten fanns förslag om att upprätta ett svenskt institut för IT-säkerhet

som kan certifiera säkerheten hos IT-produkter och IT-system samt att stärka det sektorsgemensamma och samhällsövergripande arbete som olika myndigheter utför.

### 4.3.3 1990-talet – Internet: möjligheter och problem

#### **Hot och riskutredningen och beredskapen mot svåra påfrestningar**

Försvarsdepartementet fick i december 1992 i uppdrag av regeringen att tillkalla en kommitté med uppgift att utreda påfrestningar och risker i det fredstida samhället och vissa frågor inom totalförsvarets civila del. Kommittén tog namnet "Hot- och riskutredningen". I utredningens huvudbetänkande "Ett säkrare samhälle" (SOU 1995:19) behandlades bland annat störningar i datasystem.

Utredningen ansåg att det behövde vidtas flera åtgärder inom området datasystemsäkerhet för att samhället ska uppå en så hög robusthet att det kan motstå påfrestningar av olika slag. Denna datasystemsäkerhet borde vara grundad på den fredstida säkerhetsnivån.

Utredningen föreslog att det i målen för beredskapsmyndigheternas verksamhet i krig skulle anges vilka krav på datasystemsäkerhet som skulle gälla inom de delar av verksamheten som är beroende av datorstöd. Man påpekade att det var viktigt att den som fastställde kraven även beaktade målen för den fredstida verksamheten.

Utredningen ansåg att det kunde finnas skäl sitt se över fördelningen av ansvaret mellan myndigheter som arbetar med frågor om datasäkerhet. Man föreslog att en av myndigheterna, nämligen ÖCB, borde få i uppgift att utarbeta underlag för en helhetssyn på säkerheten i viktiga datorsystem i samhället. ÖCB skulle följa utvecklingen inom datorsystemsäkerheten och rapportera iakttagelser till regeringen. I uppgiften borde även ingå att pröva om det finns mål formulerade för störda förhållanden och att bedöma på vilket sätt och i vilken utsträckning dessa mål är uppfyllda.

För att underlätta värderingen av en verksamhets datorsystemsäkerhet föreslogs att man skulle överväga någon form av certifieringsprocedur, som med utgångspunkt i en fastställd standard anger om en bestämd nivå på funktionsförmågan kommer att kunna uppnås. Certifieringen skulle kunna utgå från befintliga ISO-standarder och branschstandarder med tillägg för robusthet.

ÖCB fick också i december 1995 i uppdrag av regeringen att utreda förutsättningarna för att utforma ett system för certifiering av ADB-säkerhet som gör det möjligt att värdera hur väl ett åtagande om funktionsförmåga är uppfyllt.

#### **Proposition 1996/97:11 Beredskapen mot svåra påfrestningar på samhället i fred**

Proposition 1996/97:11 redovisade regeringens ambitioner mot svåra påfrestningar på samhället i fred med utgångspunkt från Hot- och riskutredningens arbete. Regeringen föreslog i propositionen ett antal åtgärder med avseende på säkerhet i samhällsviktiga system. Säkerhet i samhällsviktiga system betecknas i propositionen som ett område där det bör finnas en särskilt hög ambition för beredskapen.

Man rapporterade att ÖCB fått uppdraget att utreda förutsättningarna för ett system för certifiering av datasystemsäkerhet, men att detta ska utredas ytterligare.

Regeringen föreslog att en arbetsgrupp skulle tillsättas med uppdraget att följa utvecklingen av hot och risker inom informationskrigföring, sprida kunskap om detta samt lämna förslag till hur ansvar inom området skall preciseras och hur riktlinjerna för en strategi borde se ut.

Dessutom föreslogs att berörda myndigheter skulle få i uppdrag att studera aktiva åtgärder inom informationskrigföring. I propositionen påpekades att området informationskrigföring innefattar betydligt mer än bara IT-säkerhetsfrågor.

### **Statskontoret och den svenska delen av Internet**

Statskontoret jobbade tidigt med frågor rörande datorer:

”Statskontoret was founded in 1680 by the late King Charles XI. Data processing was added to its program later. In fact, matematikmaskinnämnden – the Swedish Board for Computing Machinery – was merged into Statskontoret as late as 1963.”<sup>55</sup>

Man hade 1986 presenterat en undersökning av vilka effekter mer omfattande störningar i statlig ADB-verksamhet kan få för myndigheterna och samhället i stort<sup>56</sup>.

Regeringen gav i september 1996 Statskontoret i uppdrag att utreda den svenska delen av Internet. En del av arbetet var att undersöka behovet av och förutsättningarna för att öka säkerheten i den svenska delen av Internet. Syftet med uppdraget var bland annat att minska nätets sårbarhet för störningar. Statskontoret presenterade 1997 resultatet av utredningen i sin rapport ”Svenska delen av Internet” (1997:18).

Statskontoret konstaterade att Internet måste jämföras med andra samhällsviktiga funktioner och fungera inom landet vid svåra påfrestningar på samhället både i fred och i krig. Som en konsekvens av detta ansåg Statskontoret att den svenska delen av Internet måste kunna fungera utan att vara beroende av funktioner placerade utanför Sverige.

Statskontoret föreslog ett antal åtgärder, bland annat:

- Att nationella knutpunkter och nätdata-baser skulle placeras i skyddade berggrum,
- Att utreda införande av en funktion för incidenthantering,
- Att det skulle utpekas en organisation för krishantering för Internet på nationell nivå,
- Att inrätta rutiner för att snabbt kunna isolera den svenska delen av Internet.

Dessutom kom Statskontoret med ett antal synpunkter och rekommendationer. Dessa inkluderade:

- Att kritiska noder i systemet bör ha tillgång till reservkraft för att klara elavbrott på upp till två veckor,
- Att ett grundläggande krav på samtliga Internetoperatörer är att ha en dokumenterad och verifierad kontinuitetsplan, och att detta skall kontrolleras av en myndighet,
- Att det finns ett behov av att analysera leverantörsberoendet av vitala komponenter,
- Att det är viktigt att varje operatör på den svenska marknaden har en etablerad organisation,
- Att myndigheter med ansvar för kunskaps- och informationsinhämtning inom säkerhetsområdet stimuleras till samordning,
- Att försvarets funktion för testning av krypteringsalgoritmer även utnyttjas för civila ändamål.

<sup>55</sup> Ur missiv till ur “Provisional compendium on Automatic Data Processing” av Olof Dopping, Statskontoret, 1964.

<sup>56</sup> Sårbarhet och säkerhet i statlig ADB-verksamhet, konsekvenser och störningar, Statskontoret, 1986:3

### **Statskontoret - Sammanhållen strategi för samhällets IT-säkerhet**

Regeringen gav 1997 Statskontoret ytterligare ett uppdrag; att utarbeta en sammanhållen strategi för samhällets IT-säkerhet. Denna redovisades i en rapport<sup>57</sup> av Statskontoret året därefter.

Statskontoret påpekade i rapporten att utgångspunkten för strategin om informationssäkerhet borde vara att varje organisation ansvarar för att den egna informationsbehandlingen sker med betryggande säkerhet. Strategins övergripande mål borde vara att samhällsviktiga funktioner och kritiska infrastrukturer ska skyddas och fungera störningsfritt. Statskontoret påpekade att det är staten som har det övergripande ansvaret för alla samhällsviktiga funktioner.

Ett antal förslag till åtgärder presenteras också i strategin. För att möjliggöra en bred samverkan inom området informationssäkerhet föreslog Statskontoret att ett rådgivande organ med representanter från såväl privat som offentlig sektor skulle skapas och knytas till regeringen.

Statskontoret ansåg att ÖCB borde få ansvaret för att samordna samhällets arbete med informationssäkerhetsfrågor och att ÖCB borde få ansvaret för en incidentrapporteringsfunktion. Statskontoret ansåg även att alla myndigheter, ansvariga för system eller information av samhällsviktigt slag borde åläggas att årligen inkomma med risk- och sårbarhetsanalyser till ÖCB.

På sikt ansåg Statskontoret att alla samhällsviktiga funktioner skulle vara certifierade med avseende på säkerhet, kvalitet och tillgänglighet. Certifiering av informationssäkerhet skulle gälla avseende teknisk IT-säkerhet, respektive certifiering av nivån på informationssäkerheten i en organisation. FMV nämndes som en aktör med möjlighet att erbjuda certifiering avseende teknisk IT-säkerhet. Enligt rapporten angav FMV att de på ca ett år skulle kunna erbjuda certifiering av produkter och tjänster för IT-säkerhet.

### **Ag IW**

Ag IW – arbetsgruppen om informationskrigföring – tillsattes inom regeringskansliet i december 1996 enligt förslag i propositionerna 1996/97:4 och 1996/97:11. Uppdraget var att följa utvecklingen av hot och risker inom området informationskrigföring, sprida kunskap om detta samt att lämna förslag till hur ansvar inom området skall preciseras och hur riktlinjerna för en strategi inom området bör se ut. Arbetet utfördes ungefär samtidigt med Statskontorets utredning och uppgifterna överlappade delvis. Skillnaden var huvudsakligen att fokus i Statskontorets utredning var framtida IT-incidenter medan Ag IW arbetade med den nationella säkerheten som utgångspunkt.

I augusti 1998 presenterade Ag IW i sin Rapport 2<sup>58</sup> en strategi och ansvarsfördelning för skydd mot informationskrigföring. Förslaget hade stora likheter med det som Statskontoret hade presenterat. Ag IW förordade en samordningsgrupp på hög nivå inom Regeringskansliet. ÖCB skulle ges en nationellt samordnande roll. Ag IW föreslog dock att PTS, inte ÖCB, skulle ansvara för en incidenthanteringsfunktion (StatsCERT) även om ÖCB skulle ha ansvaret för analys av incidenter. Dessutom föreslog Ag IW att det skulle inrättas en nationell aktiv IT-kontrollgrupp med Försvarsmakten som bas. Denna grupp skulle genom kontrollerande prövning av statsförvaltningens system bidra till att höja IT-säkerheten.

<sup>57</sup> Sammanhållen strategi för samhällets IT-säkerhet, Statskontoret, 1998:18.

<sup>58</sup> Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning m m. Rapport nr 2 (öppen) från arbetsgruppen om informationskrigföring. Ag IW, 1998-08-19



#### 4.3.4 2000-talet – Myndighetsansvar fördelas

##### SOU 2001:41 Säkerhet i en ny tid

Försvarsdepartementet fick i december 1999 i uppdrag av regeringen att tillkalla en särskild utredare med uppdrag att analysera och lämna förslag till principer för en bättre helhetssyn vid planeringen av civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred. Åke Pettersson förordnades som särskild utredare i mars 2000 och utredningen tog namnet Sårbarhets- och säkerhetsutredningen.

Utredningen blev klar 2001 och ägnade bland annat ett kapitel i sin rapport<sup>59</sup> åt en strategi för ökad IT-säkerhet och skydd mot informationsoperationer. Utredningen presenterade där en övergripande strategi som byggde på propositionen *Ett informationssamhälle för alla*<sup>60</sup>. Därefter föreslog utredningen ett antal statliga funktioner som man ansåg skulle inrättas och hur ansvaret för dessa skulle fördelas mellan olika myndigheter.

Konkret var det fyra nya funktioner som utredningen föreslog:

- En funktion för samordning på nationell nivå av åtgärder mot allvarliga IT-relaterade hot och IT-incidenter. Denna funktion skulle upprättas i Regeringskansliet.
- En funktion för kvalificerad omvärldsbevakning och omvärldsanalys inom IT-säkerhetsområdet. Denna funktion skulle placeras hos den av utredningen föreslagna planeringsmyndigheten. Planeringsmyndigheten skulle även få ett sammanhållande ansvar för samhällets IT-säkerhet.
- En funktion för hantering av IT-incidenter (bevakning, statistik och varning av berörda systemägare). Denna skulle inrättas som en egen myndighet i högskolemiljö med PTS som chefsmyndighet.
- En teknikkompetensfunktion inom IT-säkerhetsområdet (expert och stödfunktion med hög teknisk kompetens). Denna skulle upprättas som en egen myndighet med FRA som chefsmyndighet.

Dessutom föreslog utredningen att man skall inrätta ett system för säkerhetsinriktad evaluering och certifiering av IT-produkter och IT-system. Detta skulle vara en uppgift för FMV.

##### Proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret

Regeringen ansåg i propositionen att det behövdes en övergripande strategi för samhällets hantering av informationssäkerhet. Baserat på bland annat Sårbarhets- och säkerhetsutredningens rapport konstaterade regeringen att det finns ett behov åtgärder och att ansvars- och rollfördelningen måste fastställas. Ett viktigt förslag i propositionen var att ÖCB skulle läggas ned. Istället borde en ny myndighet inrättas med samordnande planeringsuppgifter avseende beredskap mot svåra påfrestningar på samhället i fred och civilt försvar.

Regeringen ansåg att den tvärsektoriella samordningen för informationssäkerhet och skydd mot informationsoperationer måste stärkas. Liksom Sårbarhets- och säkerhetsutredningen ansåg regeringen att:

- Den nya planeringsmyndigheten borde ges ett sammanhållande myndighetsansvar för samhällets IT-säkerhet och genomförande av övergripande omvärldsanalyser inom området.
- Det borde införas en funktion för IT-incidenthantering.
- Det borde inrättas en funktion för teknikkompetens inom IT-säkerhet.

<sup>59</sup> SOU 2001:41 Säkerhet i en ny tid

<sup>60</sup> Proposition 1999/2000:86 Ett informationssamhälle för alla

- Det borde inrättas ett system för evaluering och certifiering av IT-produkter och IT-system.

Regeringen angav dock i propositionen inte närmare hur detta organisatoriskt skulle lösas utan aviserade att man avsåg återkomma i den frågan senare under våren 2002.

### **Proposition 2001/02:158 Samhällets säkerhet och beredskap**

I proposition 2001/02:158 presenterades så den organisatoriska strukturen för samhällets informationssäkerhet vilket hade utlovats i proposition 2001/02:10. För att snabbt kunna stärka säkerheten ansåg regeringen att de fyra föreslagna verksamhetsområdena skulle fördelas på de myndigheter som hade mest näraliggande verksamhet. Förslaget innebar följande:

- Krisberedskapsmyndigheten gavs ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. I detta ingick att årligen följa och utvärdera informationssäkerheten och årligen lämna en bedömning till regeringen. Dessutom ville regeringen ge Krisberedskapsmyndigheten ansvar för att tillse att det utvecklades ett samarbete mellan offentlig sektor och näringsliv inom området.
- Post- och telestyrelsen gavs i uppgift att ansvara för hantering av uppgifter om IT-incidenter.
- Försvarets radioanstalt gavs ansvar att tillhandahålla teknikkompetens inom informationssäkerhetsområdet.
- Försvarets materielverk fick i uppgift att bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter.

Regeringen föreslog också att en utvärdering av strukturen skulle göras två år efter införandet.

## 5 Slutord

I detta arbete har det gjorts en översiktlig beskrivning av det nationella säkerhetsarbetet för tre olika infrastruktursystem. Huvudsyftet med studien är därmed uppfyllt. Dock kan det vara på sin plats att så här i sista kapitlet lyfta blicken något och försöka identifiera några viktiga faktorer som påverkat hanteringen av säkerhetsarbetet på nationell nivå inom de olika systemen.

De tre behandlade infrastruktursystemen har en del likheter, men är ändå till karaktären väldigt olika. Detta gör det vanskligt att försöka definiera några gemensamma faktorer som påverkat säkerhetsarbetet för samtliga tre system. Ett sådant försök resulterar lätt i luftigt definierade begrepp och långsökta beskrivningar av vad som är gemensamt. Däremot finns det händelser, trender och skeenden som har haft en stor påverkan på det nationella säkerhetsarbetet och som är viktiga att omnämna. De har i vissa fall kanske bara påverkat säkerhetsarbetet i två av områdena, medan det tredje kanske påverkats ur en annan aspekt som inte resulterat i att några speciella förändringar i säkerhetsarbetet.

En tydlig faktor som har påverkat det nationella säkerhetsarbetet är *elektronikens och datorernas utveckling* under den studerade perioden. Datorerna har blivit mindre, snabbare, lättare att arbeta med och mer tillgängliga. För informationsförsörjningen är det naturligtvis den enskilt största faktorn som har lett till allt större uppmärksamhet för området genom åren. Systemen har blivit öppnare för användare men även för logiska hot och *angrepp med IT-vapen*, vilket har motiverat ett ökat intresse på nationell nivå. Datorernas utveckling har även påverkat telekommunikationerna som i takt med att de digitaliserats möjliggjort nya lösningar och skapat behov av nya skyddsåtgärder. Även elförsörjningen har påverkats av denna utveckling, då framförallt eftersom samhället blivit mer beroende av kontinuerlig elförsörjning till datorerna. Acceptansen för kortare avbrott har sjunkit och detta ställer allt högre krav på en säker elförsörjning.

Under mitten av 80-talet uppmärksammades *hot från sabotageförband*. Detta gav stort genklang på nationell nivå framförallt i säkerhetsarbetet för elförsörjningen och telekommunikationerna. Detta ledde till satsningar på skydd mot sabotage. Inom elförsörjningen initierade detta även annat arbetet med att utveckla en förmåga till ö-drift samt en ökad satsning på reservkraft.

Under slutet av 80-talet kom ett nytt hot i form av *luftburna precisionsvapen*. Detta ledde till ökat fokus på fysiskt skydd för vitala delar av systemen inom framförallt telekommunikationer och elförsörjning.

*Det kalla krigets slut* och den därpå följande breddade hotbilden har haft en stor påverkan på det nationella säkerhetsarbetet inom alla tre systemen. Fokus skiftade från storskalig militär invasion till småskaliga men mer riktade attacker. Hotet från luftburna precisionsvapen fanns kvar och dessutom tillkom terroristhotet. Arbetet med den nationella infrastrukturens säkerhet uppmärksammades under 1990-talet allt mer utförligt i regeringens propositioner.

*Ansvarsfördelning och organisatorisk struktur* har varit relativt likartad för elförsörjning och telekommunikationerna. Det har funnits en myndighet som har haft sektors- eller funktionsansvar. Detta har inneburit god kunskap om systemen och att man kunnat arbeta med säkerhetsfrågor för varje system efter en sammanhållen strategi. Speciellt tydligt är detta före 1990-talets marknadsreformer, då de statliga verk som ägde stora delar av systemen för telekommunikationer (Televerket) och elförsörjningen (Statens vattenfallsverk) även hade ansvaret för det nationella säkerhetsarbetet.

Efter *marknadsreformerna* på 1990-talet minskade statens direkta inflytande över telekommunikationerna och elförsörjningen. Detta är troligen ytterligare en förklaring till att man från regeringsnivå under och efter 1990-talet blivit mer detaljerad i sina propositioner rörande säkerhets- och beredskapsfrågor inom den civila infrastrukturen.

För informationsförsörjningen har *avsaknaden av en ansvarig myndighet* varit påtaglig. Av regeringen tillsatta utredningar var fram till 90-talets början hemvist för arbetet med säkerhetsfrågor på nationell nivå. Överstyrelsen för ekonomiskt försvar och senare överstyrelsen för civil beredskap hade visserligen ett beredskapsansvar men var helt fokuserade på höjd beredskap och krig, och då mer ur en försörjningssynpunkt. Från mitten av 90-talet arbetade en mängd myndigheter med frågan vilket resulterade i att ansvaret spreds på flera händer.

Att *samhället blir mer och mer beroende* av den tekniska infrastrukturen konstaterades av SSLP redan på 1970-talet. Denna trend håller i sig än idag och beroendet kommer säkerligen inte att minska framöver.

## Referenser

Den automatiska databehandlingens teknik, Kommittén för maskinell databehandling, Finansdepartementet, SOU 1961:60

Automatisk Databehandling betänkande avgivet av kommittén för maskinell databehandling, SOU 1962:32

Provisional compendium on Automatic Data Processing, O. Dopping, Statskontoret, 1963

SOU 1969:25 Planering och programbudgetering inom försvaret, Betänkande angivet av försvarsdepartementets programbudgetgrupp, 1969-04-30

ADB-säkerhet : ADB säk. : provisoriska anvisningar för sekretess- och säkerhetsskydd vid maskinell databehandling, Industrins försvarsbyrå, 1970

ADB vid beredskap, Industrins försvarsbyrå, 1972

Dataskydd. Delrapport från Statskontorets dataskyddsprojekt, T. Gut, T. Magnusson, Statskontoret Rapport 1975:9

Datasäkerhet: hot och brister vid datordrift : rapport från en genomförd studie / av personal från Statskonsult AB - som arbetat på uppdrag av Statskontoret - och från IBM Svenska AB, 1976

Svensk samhällsutveckling: [RES rapport]. Telekommunikationerna. Försvarsdepartementet. Sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret (SSLP), 1976

Svensk samhällsutveckling: [RES rapport]. Datorerna. Försvarsdepartementet. Sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret (SSLP), 1976

Programplan 1977/78 - 1981/82 för beredskapsverksamheten beträffande försörjningen med elkraft, Statens vattenfallsverk, 1976-09-27.

Datorerna och samhällets sårbarhet. A. Eriksson, J. Freese och L. Johansson (red), 1976

ADB-säkerhet – I dag och i morgon. Dokumentation från en konferens om ADB-säkerhet 18 – 19 november 1976, Nynäshamn

Proposition 1976/77:74 om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling

ADB-säkerhet; Kontroller vid ADB. Rapport från ADB-säkerhetsprojektet vid Statskontoret, Rapport 1979:11, Dnr 359/74-5, 1979-05-15

Ds Fö 1978:4, ADB och samhällets sårbarhet, Lägesrapport från sårbarhetskommittén (SÅRK), 21 juni 1978

ADB-säkerhet: Kontroller vid ADB, Rapport från Statskontorets ADB-säkerhetsprojekt, 1979:11

SOU 1979:93, ADB och samhällets sårbarhet; Överväganden och förslag, Betänkande av sårbarhetskommittén (SÅRK), 5 december 1979

Samhällets sårbarhet i dataåldern, N. Fredholm, 1979

Det ekonomiska försvarets programplan 1982/83 – 1986/87, Överstyrelsen för ekonomiskt försvar, 1981-08-27

Studier om säkerhetspolitik och långsiktig planering: en skrift tillägnad Lennart Grape, Sekretariatet för säkerhetspolitik och långsiktplanering inom totalförsvaret (SSLP), 1981

Proposition 1981/82:102 om säkerhets och försvarspolitiken samt totalförsvarets fortsatta utveckling, 1982-02-24

Elförsörjningens sårbarhet, Per Molander, Försvarets forskningsanstalt, FOA Rapport AH 10012-M2 (Hemlig), december 1982

Vattenfall under 75 år, Statens Vattenfallsverk, 1984

Perspektivstudie fas A inför 1987 års försvarsbeslut – Behov av åtgärder i ett digitalt telenät, Televerket, 1984-06-08

SOU 1984:69 Säker elförsörjning, Betänkande av kommissionen om elförsörjningens säkerhet

Elsystemets sårbarhet, PM till sekreteraren för FK 84, ÖEF/Vattenfall, 1984-09-12

Elsystemets sårbarhet, B. Åqvist, Beredskapssektionen, Vattenfall, Föredragning PM för FK -84, 1984-12-19

Perspektivstudie fas B inför 1987 års försvarsbeslut – Behov av åtgärder i ett digitalt telenät. Televerket, september 1985

ADB i kris och krig, Sårbarhetsberedningen (SÅRB), 1985:1

SOU 1986:12, Datorer sårbarhet säkerhet, En slutrapport från Sårbarhetsberedningen (SÅRB), 1986

SKRIK 10. SKRIK-Projektet. Studier av samhället i beredskap och krig. En översikt. M. Nyberg, J-E. Svensson, FOA Rapport C10280 – 1.2, september 1986

Sårbarhet och säkerhet i statlig ADB-verksamhet, konsekvenser och störningar, Statskontoret, 1986:3

Programplan – Beredskapsåtgärder i televerkets nät 1987/77 – 1991/92, Televerket, juli 1986.

Proposition 1986/87:95 Totalförsvarets fortsatta utveckling, 1987-02-26

Central Säkerhetsplan (CS) för Televerkets säkerhetsverksamhet 1990 – 1992, Televerket, Säkerhetssektionen, april 1989

Svenska telegrafverket : historisk framställning. Bd 6, Telefon, telegraf och radio 1946-1965, H. Heimbürger, K. V. Tahvanainen, 1989

Civildepartementet Ds 1990:43, ADB och samhällets säkerhet på 90-talet. De verksamhetsansvarigas säkerhetsansvar, Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS), 1990-05-31

Civildepartementet Ds 1990:44, ADB och samhällets säkerhet på 90-talet. Samhällsaspekter på säkerhet inom betalningsväsendet, Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS), 1990-05-31

Civildepartementet Ds 1990:45, ADB och samhällets säkerhet på 90-talet. Datakriminalitet i Sverige, Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS), 1990-05-31

Civildepartementet Ds 1990:46, ADB och samhällets säkerhet på 90-talet. Strukturfrågor och säkerhet, Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS), 1990-05-31

Civildepartementet Ds 1990:47, ADB och samhällets säkerhet på 90-talet. Datakommunikation och säkerhet, Samrådsgruppen för samhällets säkerhet inom dataområdet (SAMS), 1990-05-31

Programplan 1992 – 1996 funktionen Telekommunikationer, Televerket, augusti 1990

Proposition 1990/91:102 om verksamhet och anslag inom totalförsvaret under budgetåret 1991/92, 1991-02-14

Proposition 1991/92:102 Totalförsvarets utveckling till och med budgetåret 1996/97 samt anslag för budgetåret 1992/93

ADB-säkerhet i Sverige: Vad som gjorts och vad som pågår – Resultat av inventering februari 1992, ÖCB och Statskontoret, 1992-04-27

I fädrens spår, A. Kaijser, Carlssons Bokförlag ,1994

SOU 1995:19, Ett säkrare samhälle, Huvudbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:20, Utan el stannar Sverige, Delbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:21, Staden på vattnet utan vatten, Delbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:22, Radioaktiva ämnen slår ut jordbruk i Skåne, Delbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:23, Brist på elektronikkomponenter, Delbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:24, Gasmoln lamslår Uppsala, Delbetänkande av Hot- och Riskutredningen, 1995-01-11

SOU 1995:51, Elsförsörjningen i ofred. Delbetänkande av Ellagstiftningsutredningen

Proposition 1996/97:4 Totalförsvaret i förnyelse – etapp 2, 1996-09-12

Proposition 1996/97:11 Beredskapen mot svåra påfrestningar på samhället i fred, 1996-09-12

Åtgärder och skydd mot informationskrigföring. Rapport nr 1 från arbetsgruppen om informationskrigföring. Ag IW, 1997-08-15

Svenska delen av Internet, Statskontoret 1997:18

Svenska telegrafverket : historisk framställning. D. 7, Från myndighet till bolag: 1966-1993, Sven Lernevall, Bengt Åkesson, 1997

Sammanhållen strategi för samhällets IT-säkerhet, Statskontoret, 1998:18

Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning m m. Rapport nr 2 (öppen) från arbetsgruppen om informationskrigföring. Ag IW, 1998-08-19

Sveriges militära satsningar: en översikt med förklaringar till perioden efter 1945, K. Pallin, FOA-R--98-00828-170--SE, september 1998

Regeringens skrivelse 1998/99:33 Beredskapen mot svåra påfrestningar på samhället i fred, 1998-12-10

Proposition 1998/99:74 Förändrad omvärld – Omdanat försvar, 1999-03-04

Sårbarhet i de civila telekommunikationerna, U. Pettersson, P. Wulff, G. Fischer, FOA-R--99-01221-240--SE, oktober 1999.

SOU 1999:55 Konvergens och förändring – Samordning av lagstiftningen för medie- och telesektorerna , 1999-04-01

Proposition 1999/2000:30 Det nya försvaret, 1999-11-18

Proposition 1999/2000:86 Ett informationssamhälle för alla, 2000-03-28

Regeringens skrivelse 2000/01:52 Beredskapen mot svåra påfrestningar på samhället i fred, 2000-11-14

TEBIT – Teknisk beskrivningsmodell för IT-vapen, M. Karresand, FOI-R--0305--SE, augusti 2001

SOU 2001:41 Säkerhet i en ny tid. Sårbarhets- och säkerhetsutredningen.

Proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret, 2001-09-26



Proposition 2001/02:158 Samhällets säkerhet och beredskap, 2002-03-14

När blir en avgrävd telekabel ett säkerhetspolitik problem? Inträdesanförande i Kungl Krigsvetenskapsakademien avd V den 21 februari 2002 av generaldirektör N. G. Billinger, Kungliga Krigsvetenskapsakademiens Handlingar och Tidskrift 2002

Stamnätet under ett sekel. Berättelsen om hur det svenska stamnätet byggdes upp, P. Stymne, Svenska Kraftnät, februari 2002.

De byggde Internet i Sverige, I. Hamngren och J. Odhnoff, oktober 2003

Energiläget i siffror 2003, Statens energimyndighet, 2003

Energiläget 2003, Statens energimyndighet, 2003

