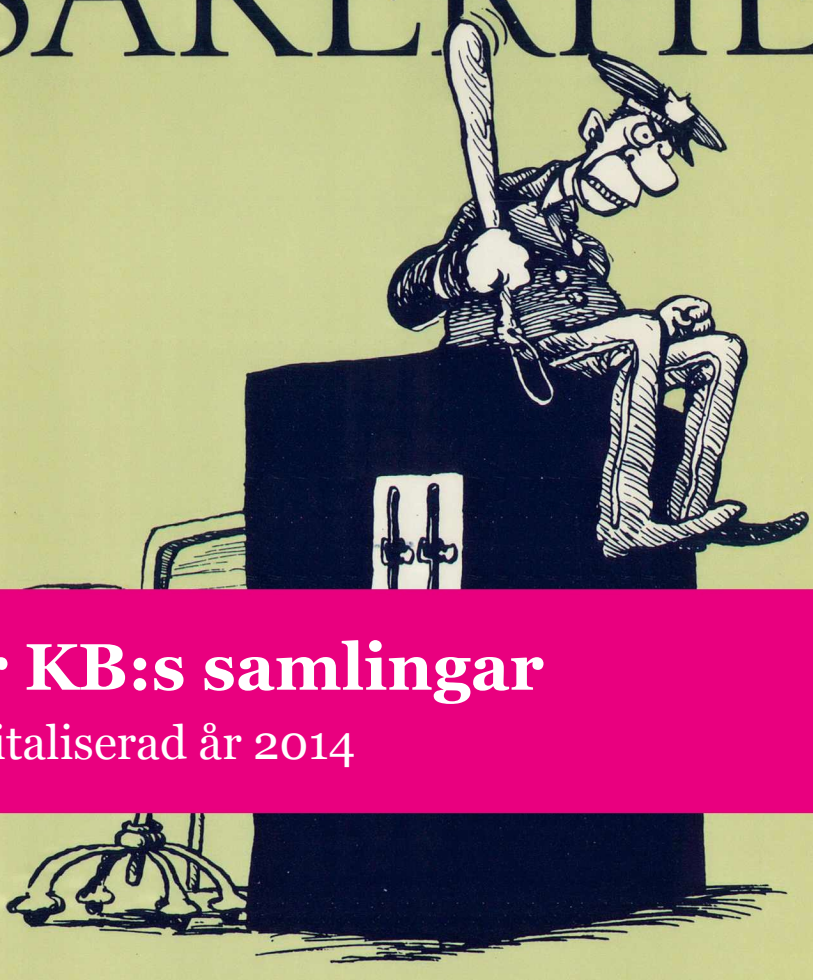
DATORER SÅRBARHET SÄKERHET



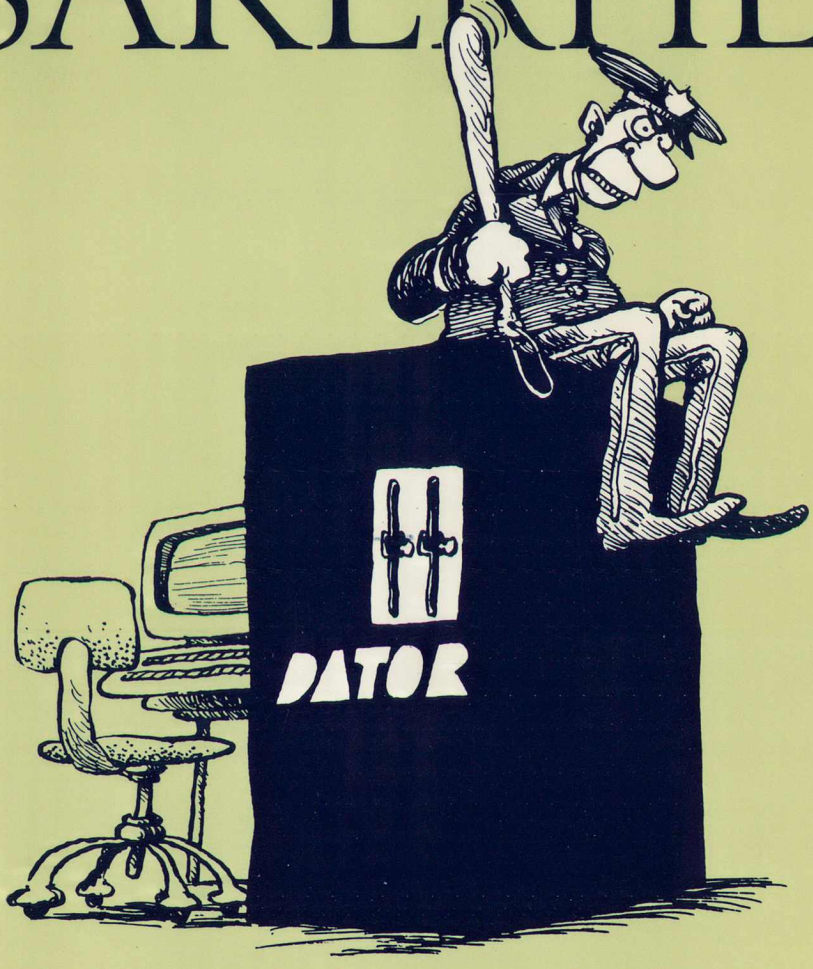
Ur KB:s samlingar
Digitaliserad år 2014

KUNGL. BIBLIOTEKET
National Library of Sweden

En slutrapport
från SÅRB

SOU 1986:12

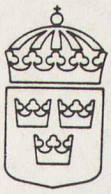
DATORER SÅRBARHET SÄKERHET



En slutrapport
från SÅRB

SOU 1986:12

124



Statens offentliga utredningar
1986:12
Försvarsdepartementet

Datorer sårbarhet säkerhet

Sårbarhetsberedningen

En slutrapport från SÅRB

Stockholm 1986

Omslagsteckning Erik Foseid
ISBN 91-38-09198-4
ISN 0375-250X

gotab Stockholm 1986 84539

Till
Statsrådet och chefen för försvarsdepartementet

Genom beslut den 23 juli 1981 bemyndigade regeringen chefen för försvarsdepartementet att tillkalla en beredning med högst 10 ledamöter för utredning och för information och rådgivning i frågor rörande säkerhet och sårbarhet på dataområdet.

Genom beslut den 20 juni 1984 erhöll beredningen tilläggsdirektiv varvid chefen för försvarsdepartementet bemyndigades att utöka beredningen till högst 12 ledamöter.

Med stöd av dessa bemyndiganden förordnade departementschefen ledamöter och sakkunniga i beredningen vars sammansättning och sekretariat framgår av bil 5.

Beredningen antog namnet sårbarhetsberedningen (SÅRB):

I enlighet med sina direktiv fastställde beredningen den 16 december 1981 en handlingsplan som beredningen anmodats inlämna till regeringen före årsskiftet 1981/82.

SÅRB har därefter i allt väsentligt följt denna handlingsplan. Arbetet har bedrivits i projektform och mestadels i samarbete med statliga myndigheter, kommuner och landsting samt organisationer och företag inom det privata näringslivet.

En huvuduppgift för SÅRB har varit att genom information och rådgivning verka för en minskad sårbarhet. I enlighet härmed har beredningen valt att efter hand offentliggöra och till en större krets distribuera sina utredningsresultat. De publicerade rapporterna framgår av bil 3.

SÅRB får härmed överlämna sin slutrapport. Den innehåller utöver en sammanfattning av de tidigare redovisade utredningsreultaten de slutsatser och rekommendationer som de olika projekten gett anledning till.

Uppdraget är härmed slutfört.

Reservation har avgivits av ledamöterna Axelsson och Svenonius.

Stockholm i januari 1986.

Allan Eriksson

Benny Andersson	*Göran Axelsson*	*Ulf Carlsson*
Johan Essén	*Jan Freese*	*Per Hoving*
Bruno Lundberg	*Orvar Lundberg*	*Bengt-Erik Nilsson*
Per Svenonius	*Per-Gunnar Vinge*	

/Thomas Osvald

Förkortningslista

ADB	Automatisk databehandling
ANSI	American National Standards Institute
BKS	Behörighetskontrollsystem
BRÅ	Brottsförebyggande rådet
CAD/	Computer Aided Design
CAM	Computer Aided Manufacturing
CFD	Centralnämnden för fastighetsdata
DAFA	Datamaskincentralen för administrativ databehandling
DALK	Datalagstiftningskommittén
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DOK	Data- och offentlighetskommittén
DS	Departementsserie
EMP	Elektromagnetisk puls
FAR	Föreningen Auktoriserade Revisorer
FIPS	Federal Information Processing Standard
FOA	Försvarets forskningsanstalt
FRI	Försvarets rationaliseringsinstitut
ISO	International Organisation for Standardisation
LKD	Leverantörföreningen Kontors- och Datautrustning
PTS	Postens Transportstyrningssystem
RDF	Riksdataförbundet
RPS	Rikspolisstyrelsen
RRV	Riksrevisionsverket
RSF	Remote Support Facility
RöS	Röjande signaler
SAF	SVenska arbetsgivareföreningen
SBA	Sårbarhetsanalys
SCB	Statistiska Centralbyrån
SHB	Svenska Handelsbanken
SHIO	Sveriges hantverks- och industriorganisation-Familjeföretagen
SIG/SEC	Särskild intressegrupp för ADB-säkerhet inom SSI
SIS	Standardiseringskommissionen i Sverige
SOU	Statens offentliga utredningar
SPADAB	Sparbankernas Datacentraler AB
SSI	Svenska samfundet för informationsbehandling
STU	Styrelsen för teknisk utveckling
SÅRB	Sårbarhetsberedningen
SÅRK	Sårbarhetskommittén
VPC	Värdepapperscentralen
ÖB	Överbefälhavaren
ÖEF	Överstyrelsen för ekonomiskt försvar

Innehåll

1 Sammanfattning

Inledning

SÅRB har under åren efter hand offentliggjort och till en större krets distribuerat sina utredningsresultat. I denna slutrapport redogör beredningen för de slutsatser och rekommendationer som de olika projekten gett anledning till. En fylligare redogörelse lämnas för några mindre omfattande projekt och initiativ vars resultat ej tidigare redovisats separat.

SÅRB:s tillkomst

I kapitel 2 redogörs för sårbarhetsberedningens bakgrund. År 1979 föreslog den dåvarande sårbarhetskommittén, SÅRK i sitt betänkande en sårbarhetslag för att komma till rätta med sårbarhetsproblemen. Remissinstanserna uttalade samstämmigt behovet av åtgärde. Flertalet avvisade emellertid lagstiftning.

Regeringen beslutade 1981 att tillsätta sårbarhetsberedningen, SÅRB. Man ansåg det vara angeläget att samhället fick bättre överblick och kunde ta initiativ till åtgärder för att minska sårbarheten. I stället för att tillgripa lagstiftning skulle man genom information och rådgivning öka datoranvändarnas medvetande om problemen och inspirera dem till åtgärder på frivillig väg.

SÅRB fick i sina direktiv till uppgift att inledningsvis utarbeta och för regeringen redovisa en handlingsplan för sitt arbete. I handlingsplanen tog SÅRB upp alla de projekt som sedan under åren från 1981 i allt väsentligt fullföljts.

Vilka projekt som ingick i handlingsplanen framgår av avsnittet 5.

SÅRB:s sammansättning

Sårbarhetsberedningen tillsattes av regeringen och kom att omfatta 10 ledamöter. Beredningen utökades sedermera med ytterligare två representanter för industrien. Beredningen är en expertkommitté utan politikerinslag. Ledamöterna representerar försvars- och datamyndigheter, kommun- och landstingsförbunden och näringslivet.

Avsikten var att beredningen skulle avsluta sitt arbete till den 1 juli 1984 men mandatet förlängdes i tilläggsdirektiv till utgången av 1985.

Utvecklingen efter SÅRK.

I kapitel 3 tar SÅRB bl a upp frågor om hur sårbarhetsfrågorna utvecklats under de senaste åren. SÅRB konstaterar att

- datoriseringen fortsätter i hög takt med nya tillämpningar, ny teknik och ökad integration,
- intresset för sårbarheten har ökat i massmedia, bl a som följd av ett antal incidenter med "hackers" och problem med amerikansk exportkontroll, t ex den s k containeraffären,
- medvetandet om sårbarheten ökat bl a som en följd av SÅRB:s arbete, men kanske inte ännu fått tillräckligt genomslag,
- sårbarhetsintresset delvis förskjutits från de dramatiska kriminella frågorna mot det mera vardagliga, oavsiktliga. SÅRB konstaterar att god personalpolitik, ordning och reda, utbildning osv ökar både säkerheten och effektiviteten.

Vidare redogörs för hur SÅRB bedrivit sitt arbete – i samarbete med myndigheter, kommuner, näringsliv och organisationer.

Slutligen berörs det internationella läget i fråga om ADB och sårbarhet. SÅRB konstaterar att Sverige internationellt sett har en framträdande position.

Information

I kapitel 4 redogörs för omfattningen och inriktningen av den utåtriktade rådgivnings- och informationsverksamheten som enligt SÅRB:s direktiv varit en viktig uppgift för beredningen.

SÅRB har vid ett par tillfällen gått ut till myndigheterna med påminnelse om beredningens avsedda funktion som remissinstans särskilt vad gäller större statliga ADB-system. Trots detta har någon nämnvärd remissverksamhet ej kommit till stånd.

SÅRB har under årens lopp i några fall funnit anledning att ta upp frågor som ej var förutsedda och inte nämns i handlingsplanen. Några av dessa har varit av den omfattningen att de behandlas som projekt i slutrapportens kapitel 5.

Postens transportstyrningssystem

Ett initiativ som var av mindre omfattning men ändå av principiell betydelse avser postens transportstyrningssystem, PTS. SÅRB uppmärksammade regeringen på risken för att ADB-register som är känsliga från totalförsvarssynpunkt inrättas utan prövning och utan att saken ens kommer till myndighets kännedom och förordade snara åtgärder för att förbättra statsmakternas möjligheter till överblick och påverkan av utvecklingen av ADB-användningen. Åtgärder i denna riktning har numera vidtagits.

SÅRB:s projekt

I kapitel 5 redogör SÅRB för de projekt som beredningen arbetat med. I de fall projektresultaten redan avrapporterats i separata rapporter lämnas

endast en kortfattad redogörelse för projektets innehåll, omfattning, etc. I övriga fall lämnas en mera omfattande projektredovisning. Resultatet av vart och ett av de olika projekten sammanfattas under rubriken Slutsatser och rekommendationer.

Projekten redovisas i huvudsak i den ordning de togs upp i handlingsplanen.

I avsnittet 5.1 redogörs för bakgrunden till arbetet med sårbarhetsanalys och den s k **SBA-metoden,** hur metoden har förts ut till datoranvändarna och den utvärdering av metoden som skett.

SÅRB anser att

- SBA bör modifieras med ledning av hittills vunna erfarenheter,
- statsmyndigheter av betydelse för totalförsvaret bör åläggas att göra sårbarhetsanalys och öka sin beredskap för bortfall av datorkraft.

Frågan om **utlandsberoendet** i 5.2 har inte tidigare redovisats i någon separat rapport. SÅRB diskuterar utlandsberoendet för olika typer av produkter i ett par olika tänkta krissituationer.

SÅRB anser att

- underlaget för en säkrare bedömning av utlandsberoendet måste förbättras genom en utredning av vilka systemdatorer som måste fungera i kris och krig och vilka vi kan undvara,
- utvecklingen måste noga följas för att förhindra att viktiga totalförsvarsfunktioner blir beroende av utländska programvaruleverantörer,
- staten bör vidta åtgärder för att underlätta och stimulera s k tredjepartservice av datorer, vid upphandling ställa särskilda krav på underhållsplanering och underhållsmässighet samt stimulera standardisering och lagerhållning på komponent- och högre nivåer. Mobiliseringsplaneringen bör ses över så att dataspecialister i erforderlig omfattning kan fortsätta i sitt yrke även under beredskap och krig.

I avsnittet om **Utslagen datorkapacitet** nämns något om bakgrunden till och slutsatserna i det projekt, som slutredovisades i SÅRB:s rapport Praktisk Katastrofplanering – val av reservdriftalternativ. I rapporten nämns de faktorer som avgör val av alternativ och vilka dessa är i olika avbrottssituationer.

SÅRB anser att

- planering för hur verksamheten skall fungera vid avbrott i databehandlingen – med reducerat datorstöd, minskad service, eliminering av ej absolut nödvändiga funktioner – måste ske i anslutning till systemutformningen.

I avsnittet om **Personrelaterade faktorer** nämns de två projekt som SÅRB genomfört och som handlar om sådana faktorer – Nyckelpersonal inom datordriften och Personal och säkerhet. Vidare redogörs för skälen till att de i handlingsplanen nämnda delutredningarna om databrott och arbetsmarknadskonflikter ej kommit till utförande.

SÅRB anser att

- frågor om beroende av nyckelpersoner och hur dataverksamheten skall organiseras och administreras för att minska sårbarheten är mycket viktiga och hittills otillräckligt utredda.

SÅRB har i en rapport om **ADB-systemens komplexitet diskuterat komplexiteten som sårbarhetsfaktor.**

SÅRB anser att

- det är nödvändigt att förändra den traditionella systemutvecklingsmetodiken – att lämna det procedurorienterade betraktelsesättet till förmån för databasorienterade utvecklingsmodeller. Sådana modeller ställer särskilda krav på datakvaliteten,
- frågor om systemkomplexitet och datakvalitet bör bli föremål för forskningsinsatser.

I avsnittet **Datakommunikation** nämner SÅRB en inom beredningen planerad rapport om datakommunikationernas sårbarhet för vilken Televerket svarar. Rapporten har ännu ej utkommit.

SÅRB anser att

- möjligheterna att avlyssna, sabotera och störa datakommunikationerna är stora,
- avlyssningsrisken måste mötas med kryptering av känsliga data,
- den som planerar och utvecklar system skall ha klart för sig vilken driftsäkerhet telenätet erbjuder och att Televerket måste lämna uppgifter härom.

I ett avsnitt om **ADB i industrin** konstateras att det projekt med detta namn som togs upp i SÅRB:s handlingsplan av olika skäl inte kommit att föranleda någon särskild utredning. Frågan om näringslivets uppgiftslämnande till staten har dock behandlats i avsnittet om Kassaskåpssäker ADB?

Projektet **Undanförsel och förstöring av register** slutfördes 1983 med ett betänkande med förslag till lagstiftning m m. SÅRB:s förslag bereds f n inom regeringskansliet.

I avsnittet **ADB i krig** nämns den rapport som SÅRB utarbetat för 1984 års försvarskommitté. I rapporten konstateras att många viktiga samhällsfunktioner är beroende av ADB och att ADB-stödet är mycket sårbart.

SÅRB anser att

- frågor om ADB i kris och krig måste behandlas ytterligare i en huvudstudie där åtgärder i en grundnivå respektive en tilläggsnivå bör övervägas,
- i en grundnivå bl a bör övervägas frågor om decentralisering av system, standardisering och lagerhållning av utrustning, kryptering, vidgad beredskapsplanering, undanförsel eller förstöring av känsliga register, åtgärder för att tillgodose personalbehovet i kris och krig samt åtgärder mot elektromagnetisk puls, EMP,
- i en tilläggsnivå bör övervägas uppbyggnad av en begränsad produktionskapacitet för elektroniska standardkomponenter och uppbyggnad av ett säkerhetsnät som överlagras det landsomfattande fiberoptiska nät som nu håller på att införas.

I ett avsnitt om **Utbildning** nämns ett kompendium för utbildning i ADB-säkerhet och sårbarhet som SÅRB tagit fram samt broschyr och affisch som distribuerats bl a till landets skolor.

I ett avsnitt om **Kryptering** nämns det projekt som SÅRB drivit i samarbete med RDF och SIS i syfte att vidga kunskapen om kryptering och som resulterat i en handbok om kryptering.

SÅRB anser att

- kraven på skydd av data som sänds via telenätet eller på magnetband snabbt håller på att skärpas. Det kommer i allt flera situationer att bli nödvändigt att tillgripa kryptering.

Röjande signaler – akustiska, elektromagnetiska eller videosignaler – som avges av datautrustning kan leda till obehörig avlyssning av databehandlingen. En skrift härom har SÅRB och BRÅ producerat.

I ett avsnitt om **Kravspecifikation i behörighetskontrollsystem BKS** nämner SÅRB sin rapport Säkerhetskrav på datorer och operativsystem som syftar till att förbättra datoranvändarnas möjligheter att ställa krav på sådana system.

SÅRB anser att

- det är viktigt att öka användarkompetensen i fråga om ADB-säkerhet
- det är viktigt att utveckla bättre ADB-säkerhetsmetoder.

I avsnittet 5.14 om **Offentlighetsprincipen, ADB och sårbarhet** beskrivs den promemoria härom som SÅRB låtit ta fram och som föranlett SÅRB att till regeringen framföra vissa förslag i syfte att minska riskerna för att offentlighetsprincipen tillämpas på ett sätt som kan skada viktiga totalförsvarsintressen.

SÅRB anser att

- överblicken över datoriseringen i samhället bör förbättras,
- riktlinjer för myndigheternas försäljning av data bör utarbetas.

I avsnittet **Kassaskåpssäker ADB?** tar SÅRB upp frågorna om sekretessbelagda data får det skydd i datorsystemen som sekretesslagen förutsätter.

SÅRB anser att

- de säkerhets- och kontrollmetoder för ADB som finns idag inte ger godtagbart skydd av hemliga eller eljest känsliga data, och att metodutveckling behövs för att förbättra skyddet,
- större restriktivitet i uppgiftsspridningen bör övervägas. Vissa uppgifter bör inte vara åtkomliga via datakommunikation och terminaler. Behörigheten att ta del av hemliga uppgifter bör begränsas.

I avsnittet **Inventering av ADB-säkerhet** redogör SÅRB för den inventering av hittillsvarande ADB-säkerhetsarbete som statskontoret gjort för SÅRB och SÅRB:s analys av inventeringen och dess resultat.

SÅRB anser att

- metodutveckling är viktig för att förbättra säkerheten och att metodutvecklingsarbetet bör fortsätta,

- den hittills tillämpade begreppsapparaten inom säkerhets- och sårbarhetsområdet är mogen för översyn och revision.

Resultat och förslag

I kapitel 6 redogör SÅRB för uppnådda resultat och framlagda förslag. De slutsatser och rekommendationer som tas upp i projektbeskrivningarna i kapitel 5 sammanfattas. I korthet innebär de följande

SÅRB anser att

- den arbetsform som beredningen valt och som innebär långtgående samarbete med myndigheter, företag och organisationer har stora ekonomiska och praktiska fördelar. Samarbetet har också ett värde i sig genom bättre förståelse och ökat förtroende mellan företrädare för olika sektorer i samhället.

SÅRB:s arbete har, som avsikten var, lett till ökat medvetande om sårbarheten och nödvändigheten av att göra något åt den. Men trycket måste bibehållas. Sårbarheten är fortfarande oacceptabel. SÅRB menar att det i mycket är en fråga om att påverka attityder och det tar avsevärd tid.

Metod- och produktutveckling på ADB-säkerhetsområdet är i dag lika nödvändig som tidigare.

I den senare delen av kapitel 6 har viktigare slutsatser och rekommendationer från projektbeskrivningarna i kapitel 5 samlats.

Då det gäller **kunskap och metoder** på säkerhetsområdet pekar SÅRB på behovet av att förnya begreppsapparaten. Bl a som en följd av den starka expansionen av datakommunikationen och de brister i fråga om skyddet som konstaterats under senare år framhålls behovet av nya och bättre säkerhetsmetoder.

Riskerna för databrott och hur de kan förhindras bör uppmärksammas mera.

SÅRB konstaterar att det är viktigt att sårbarhets- och säkerhetsaspekterna beaktas redan tidigt i systemutvecklingen. Härigenom skulle problemen med stora komplexa system som växer okontrollerat genom systemändringar och integration kunna minskas. Komplexitets- och datakvalitetsfrågorna bör f ö utredas ytterligare.

När det gäller vad utvecklingen på datorområdet för med sig och **nya förutsättningar för sårbarhet och säkerhet,** som efter hand växer fram konstaterar SÅRB att tillämpningen av offentlighetslagstiftningen och sekretesslagen fått oönskade konsekvenser. Det finns inte metoder som kan skydda sekretessbelagda uppgifter i en centraldator med kanske hundratals terminaler på samma betryggande sätt som ett pappersdokument i ett kassaskåp. Tveksamt är också om det är förenligt med sekretesslagens syfte att tilldela kanske tiotusentals tjänstemän behörighet att ta del av hemliga uppgifter. SÅRB anser att decentralisering som medel att minska angivna olägenheter borde prövas.

SÅRB menar att det finns starka skäl att stödja en strävan efter ökad kompetens och inflytande hos datoranvändarna gentemot datorleverantörerna.

Det finns ett stort behov av att närmare belysa hur det datoriserade

samhället skall fungera i kris och krig. Det är enligt SÅRB:s mening omöjligt att göra detta utan att först inhämta vetskap om vilka funktioner/datorer som är oumbärliga och vilka vi kan avstå ifrån i dessa situationer.

För att minska utlandsberoendet föreslår SÅRB ökad tredjepartservice, särskilda krav på underhållsplanering och underhållsmässighet vid upphandling, insatser för att stimulera standardisering och lagerhållning av komponenter samt översyn av mobiliseringsplanering så att personal i nyckelbefattningar inte kallas in i militärtjänst.

SÅRB anser att de statliga myndigheterna bör åläggas att genomföra sårbarhetsanalyser av sin ADB-verksamhet och utarbeta planer för hur myndighetsfunktionerna skall fullgöras i ett datorlöst tillstånd.

Vad gäller frågan om **bevakningen av sårbarhetsfrågorna i framtiden** menar SÅRB att erfarenheten visar att samhället har ett behov av överblick över datoriseringen om man vill förhindra en från totalförsvarssynpunkt olämplig och okontrollerad utveckling. Det är också enligt SÅRB:s mening nödvändigt att inte splittra den mycket begränsade kompetensen i fråga om ADB-säkerhet och sårbarhet utan hålla samman och kraftsamla resurserna för gemensam insats inom alla samhällssektorer. Slutsatsen härav är att allt talar för att samhället även framledes bör förfoga över ett organ som kan svara för allmän överblick och kraftsamling inom sårbarhetsområdet så som SÅRB hittills gjort.

2 Bakgrund

2.1 Sårbarhetskommittén, SÅRK

2.1.1 SÅRK:s förslag

Enligt beslut av regeringen tillsatte försvarsministern 1977 sårbarhetskommittén (SÅRK) med uppgift att utreda sårbarheten hos det datoriserade samhället och att föreslå åtgärder för att minska denna.

SÅRK överlämnade 1979 sitt slutbetänkande. SÅRK konstaterade att den kartläggning av förhållandena som kommittén gjort ledde fram till "den allmänna slutsatsen att sårbarheten är oacceptabelt hög i dagens genomdatoriserade samhälle. Den fortgående utvecklingen leder till en allt högre sårbarhet i framtiden om inte motåtgärder vidtas. Denna bedömning gäller både för krigs- och beredskapssituationer. Olika händelser och angrepp kan ge omfattande störningar och skador även vid djupaste fred."

För att komma tillrätta med problemen föreslog SÅRK en sårbarhetslag. Förslaget omfattade bl a följande.

- Tillståndsprövning av datoranvändning hos huvudsakligen myndigheter.
- Anmälningsplikt för vissa andra organ med verksamhet av vikt för landets försörjning.
- Aktiv rådgivnings- och informationsverksamhet.
- Tillsyn och kontroll av lagens efterlevnad.

Datainspektionen föreslogs få uppgiften som tillstånds- och tillsynsmyndighet och svara för rådgivning och information.

2.1.2 Remissyttrande över SÅRK:s betänkande

Ett stort antal myndigheter, organisationer och företag yttrade sig över SÅRK:s betänkande. Ett flertal av remissinstanserna instämde allmänt i SÅRK:s bedömning att sårbarheten var oacceptabel och att motåtgärder måste vidtas av samhällsorganen.

En övervägande majoritet var emellertid kritisk mot förslaget till sårbarhetslag och förordade i stället främst rådgivningsverksamhet. Bl a var man negativ till tillståndsförfarande som ett medel att begränsa sårbarheten och befarade en ökad byråkratisering. Viktigare var behovet av reella skyddsfunktioner snarare än den administrativa rutinen för kontroll över

datoranvändningen och dess utveckling. Många efterlyste ställningstagande till vad som kan anses utgöra en acceptabel sårbarhet. Kan man inte definiera vad som är en rimlig sårbarhetsnivå kan man heller inte fatta t ex tillståndsbeslut rörande enskilda ADB-tillämpningar.

Många ansåg SÅRK:s kartläggning av sårbarhetsfaktorer förtjänstfull. Flera ansåg särskilt att utbildning är av stor vikt för att minska sårbarheten. Kritik riktades mot den föreslagna anmälningsskyldigheten medan de allra flesta av remissinstanserna var eniga om behovet av rådgivning och information. Många menade att minskad sårbarhet främst nås genom ökat medvetande. Som ett alternativ till tillståndsförfarande angav många utarbetande av normer för hur dataverksamheten skall bedrivas i förening med en aktiv rådgivning.

2.1.3 1978 års försvarskommitté

Datasårbarheten uppmärksammades även av 1978 års försvarskommitté som i sitt slutbetänkande (DS Fö 1981:14) under rubriken överväganden och förslag avseende ekonomiska försvaret anförde:

> Kommittén vill också framhålla betydelsen av att pågående studier av datorberoendet och möjligheterna att vidta åtgärder för att nödvändig datordrift skall kunna pågå under kriser och krig fortsätter. Det är därvid enligt kommitténs mening nödvändigt att i första hand kartlägga vilka system som måste vara i drift under kriser och krig. Beredskapssynpunkter måste beaktas i hög grad när ADB-system skall införas eller moderniseras inom sektorer som har stor betydelse för totalförsvaret. Gemensamma normer bör fastställas för sådan ADB-utrustning så att kommunikation mellan ADB-system, drift och service, tekniskt skydd m m underlättas. Det bör också klarläggas hur serviceorganisation och reservdelsförsörjning bör vara organiserad.

Enligt försvarsdepartementets remissammanställning berörs det ekonomiska försvaret endast mycket kortfattat i remissvaren.

2.2 Sårbarhetsberedningen, SÅRB

2.2.1 Direktiv

I juli 1981 tog regeringen beslut om att tillsätta sårbarhetsberedningen. Regeringen hade tagit intryck av SÅRK:s konstaterande och flertalet remissinstansers instämmande i att sårbarheten hade blivit oacceptabelt hög. Det framhölls att det är angeläget att samhället får överblick och kan ta initiativ till åtgärder som syftar till ett mindre sårbart samhälle. Detta skulle också gagna vårt totalförsvar. Beträffande åtgärder för att komma till rätta med sårbarheten anfördes i direktiven följande:

> Av hänsyn till den blandade remissopinionen och till det ekonomiska läget som i allmänhet inte möjliggör några mera omfattande statliga insatser utan motsvarande omprioriteringar anser jag att man måste finna delvis andra former för att komma till rätta med sårbarheten än dem SÅRK föreslagit. Så långt möjligt bör detta ske på frivillig väg. Information och rådgivning måste därför bli ett väsentligt inslag. För detta liksom för nödvändig överblick bör samhället ta ansvar. Beträffande stora eller på

annat sätt viktiga system på den statliga sidan bör man emellertid finna sådana rutiner att en sårbarhetsprövning regelmässigt kommer till stånd som ett led i handläggningen av ärenden inför statsmakternas ställningstagande. Sårbarhet måste därvid självfallet vägas mot de andra aspekter som kan vara aktuella vid prövningen.

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
- t v 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.

2.2.2 Handlingsplanen

SÅRB fick i direktiven som nämnts i uppdrag att utarbeta en handlingsplan och en närmare precisering av vilka sårbarhetsfaktorer och sårbarhetsproblem som krävde särskild uppmärksamhet och åtgärder från samhällets sida. Handlingsplanen skulle överlämnas till regeringen i tid för att kunna prövas i samband med 1982 års totalförsvarsproposition och den datapolitiska propositionen våren 1982.

I handlingsplanen behandlas först de faktorer som enligt SÅRK påverkar det datoriserade samhällets sårbarhet. Dessa indelades av SÅRK i två huvudkategorier, yttre och inre.

Med yttre faktorer avsågs olika angrepp utifrån. Till denna kategori räknade SÅRK kriminella handlingar, missbruk för politiska syften krigshandlingar samt katastrofer och olyckshändelser. Med inre sårbarhetsfaktorer avsåg SÅRK sådana faktorer som ligger mer eller mindre inbyggda i själva datorutnyttjandet. SÅRK tog i sitt betänkande upp följande inre sårbarhetsfaktorer: innehållsmässigt känsliga register, funktionellt känsliga register, koncentration, bearbetningsmöjligheter vid ansamling av stora datamängder, bristfällig utbildning, nyckelpersoner för datordriften, dokumentation, bristande kvalitet i fråga om maskin- och programvara, katastrofberedskap, integration och inbördes beroende samt utlandsberoende.

Till dessa faktorer lades i handlingsplanen ytterligare några, nämligen ADB-systemens komplexitet, koncentration av servicebyråverksamheten och datakommunikation.

I handlingsplanen behandlas därefter de arbetsområden som SÅRB avsåg att ta itu med. Dessa överensstämmer ej helt med de som SÅRK redovisat. Vissa faktorer sammanfördes i större arbetsområden. Dispositionen påver-

kades också av vad som angivits i direktiven. Det mest omfattande arbetsområdet och det som sedermera visat sig ta i anspråk en stor del av beredningens tid och resurser var att utarbeta en metod för sårbarhetsprövning. Det fanns flera skäl till att denna väg valdes. Den alltför höga sårbarheten berodde enligt vad som framförts i SÅRK:s betänkande, i remissyttrandena och i SÅRB:s direktiv på att medvetenheten om säkerhets- och sårbarhetsproblemen i den egna verksamheten och hos samhället var låg, att intresset och kunskaperna var otillräckliga, att datoranvändarna behövde råd och hjälp att själva ta itu med sina egna sårbarhetsproblem. Mot denna bakgrund framstod det som särskilt intressant att ta fram en metod – ett hjälpmedel, som underlättade för var och en att själv analysera sin egen sårbarhet. Det är denna metod, som kom 1983, som kallas för SBA/ SårBarhetsAnalys.

SÅRB har eftersträvat att hålla fast vid och inte utan särskild anledning frångå de arbetsområden som definierades i handlingsplanen. Inom några områden har dock tiden och fortsatt utveckling ändrat förutsättningarna. I redogörelsen för de olika projekten framgår detta.

2.2.3 Handläggning av handlingsplanen

SÅRB:s handlingsplan överlämnades till chefen för försvarsdepartementet vid årsskiftet 1981/82. I regeringens proposition 1981/82 102 om säkerhets- och försvarspolitiken samt totalförsvarets fortsatta utveckling, som baseras på 1978 års försvarskommittés betänkanden framhåller försvarsministern "att det är angeläget att regeringen snarast tar initiativ till åtgärder som syftar till att minska den sårbarhet i samhället som beror på datoriseringen". Efter att ha refererat SÅRB:s handlingsplan anför departementschefen att "Jag kommer att behandla sårbarhetsberedningens handlingsprogram i den datapolitiska proposition som kommer att föreläggas riksdagen under våren".

Den datapolitiska propositionen 1981/82:123 "Samordnad datapolitik" har som centralt tema ett antal "principer och riktlinjer" för datateknikens utveckling och användning. Till den kategori ämnen, som enligt propositionen bör bli föremål för ytterligare utredning hörde bl a följande:

Näringsliv, förvaltning och arbetsliv

– – –

Säkerhet och sårbarhet

Sårbarhetsfrågorna bör ägnas kontinuerlig uppmärksamhet, inte minst inför generationsskifte av datorer och databehandlingssystem. Vid generationsskiften bör man tillvarata den tekniska utveckling som under vissa förutsättningar kan möjliggöra mindre sårbara lösningar, ofta i decentraliserad form. Ett företag eller en myndighet bör utforma sina datasystem och organisera driften på ett sådant sätt att det inte uppstår starka beroendeförhållanden till vissa nyckelpersoner inom eller utom organisationen vad gäller utveckling och drift av datorsystem.

– – –

Samhället

– – –

Databrott

Studier av databrottslighet bör genomföras för att belysa möjliga konsekvenser och behov av åtgärder.

Sårbarhet
Det fortsatta arbetet med sårbarhetsfrågorna måste syfta till att återge samhället så mycket som möjligt av den motståndskraft mot störningar som fanns före datoriseringen.

Av skäl som ligger vid sidan om syftet med denna rapport kom någon anmälan till datapropositionen såvitt avser försvarsdepartementet ej att ingå i datapropositionen. SÅRB:s handlingsplan kom därför över huvud taget inte att – som aviserades i den försvarspolitiska propositionen – tas upp till behandling och föreläggas riksdagen. Den enda reaktionen från regeringens sida utgörs i själva verket av en anteckning i ett departementsprotokoll 1982-01-07 där chefen för försvarsdepartementet meddelar att han tagit del av handlingsplanen och beslutar att planen skall läggas till handlingarna.

2.2.4 SÅRB:s sammansättning

SÅRB är liksom sin företrädare SÅRK en expertkommitté och saknar alltså politiskt inslag. Regeringen valde ledamöter i SÅRB så att dess sammansättning skulle garantera att det blev ett forum med bred representation. SÅRB består av 12 ledamöter från försvars- och datamyndigheter och datadelegationen på den statliga sidan, från kommun- och landstingsförbunden samt från näringslivet. Ursprungligen bestod SÅRB av tio ledamöter men utökades 1984 för att ge utrymme för ytterligare representation från näringslivet.

2.2.5 Tilläggsdirektiven

Avsikten var redan från början att SÅRB skulle ha ett tidsbegränsat mandat för att man därefter skulle kunna bedöma hur SÅRB lyckats och ta ställning till hur sårbarhetsfrågorna skulle hanteras i fortsättningen. Ursprungligen var avsikten att beredningen skulle avsluta sitt arbete till den 1 juli 1984 men mandatet måste på grund av sjukdom och andra oförutsedda problem förlängas genom tilläggsdirektiv till utgången av 1985.

I februari 1984 hemställde SÅRB om att få förlängd utredningstid på grund av resursproblem. I juni 1984 beslutade regeringen om tilläggsdirektiv (Dir 1984:29). Försvarsministern uttalade i direktiven att det var "mycket angeläget att de erfarenheter och det breda kunnande inom området sårbarhet/säkerhet som SÅRB besitter tas tillvara för att dels redovisa en översikt av genomfört utrednings- och utvecklingsarbete inom området ADB-säkerhet, dels analysera användbarheten av det tillgängliga materialet". I de fall SÅRB fann att kompletterande arbete borde utföras skulle SÅRB föreslå åtgärder för att komma till rätta med problemen. SÅRB skulle vidare redovisa resultaten av handlingsplanen och då främst SBA-metoden, redovisa sådant material som kunde vara av värde för försvarskommittén samt i övrigt fortsätta med information, rådgivning och remissverksamhet. Enligt de nya direktiven skulla SÅRB i sin planering utgå från att beredningens arbete skulle avslutas under år 1985.

3 Avgränsning, mål, arbetsformer

3.1 Sårbarhetens gränser och innehåll

SÅRK angav i sitt betänkande "ADB och samhällets sårbarhet" att man såg som sin uppgift att söka belysa sårbarhetsproblem förknippade med krigs – och beredskapssituationer, terrorism samt befarade missbruk för politiska syften. Man ansåg inte att kommitténs uppdrag omfattade sådan ADB som är avsedd att användas i krigföring och att försvarets ADB-verksamhet i övrigt omfattades endast i de avseenden de var jämförbara med den civila sektorns ADB-verksamhet.

SÅRB konstaterade i handlingsplanen att samhällets sårbarhet är något annat och mera än summan av de enskilda myndigheternas och företagens sårbarhet. Utvecklingen bekräftar detta. Man kan inte begära av en enskild myndighet eller ett enskilt företag att man realistiskt skall kunna bedöma i vilka avseenden, på vilket sätt och med vilken styrka den egna sårbarheten påverkar samhället och totalförsvaret. För detta behövs bl a överblick över datoriseringen. Posten har, som exempel, inte förutsättningar att helt på egen hand göra en realistisk bedömning av de eventuella skadeverkningar ett system som postens transportstyrsystem kan ha för totalförsvaret.

SÅRB nämner i handlingsplanen att inte bara avsiktliga hot mot ADB-verksamheten utan även de oavsiktliga skall innefattas i sårbarheten för att få en mera fullständig och heltäckande bild av sårbarhetsproblemen. SÅRB understryker vikten av att ett sådant mera heltäckande begrepp används. Det är svårt att dra en klar gräns mellan avsiktligt och oavsiktligt. En del av den osäkerhet som rått om definitionerna och sambanden mellan begreppen sårbarhet och ADB-säkerhet beror säkert på sådana konstlade avgränsningsförsök. ADB-säkerhet och sårbarhet är komplementära – ökar säkerheten så minskar sårbarheten och tvärtom.

3.2 Utvecklingen efter SÅRK

Det finns anledning att här något beröra frågan om hur tiden och utvecklingen kommit att påverka sårbarheten. Har den ökat eller minskat under de senaste åren, har vissa aspekter fått ökad betydelse och andra minskad?

Sedan SÅRK tillsattes för snart 10 år sedan har antalet datoriserade tillämpningar vuxit mycket starkt, åtskilliga av dem är av den arten att något

likvärdigt manuellt reservalternativ ej är tänkbart eller möjligt. I andra fall vore manuella reservalternativ tänkbara men finns inte utvecklade eller underhållna. Vidare har integrationen ökat ytterligare och därmed systemens komplexitet. Antalet datorer har ökat avsevärt liksom användningen av datakommunikation. Smådatorernas spridning har bl a haft till följd att ADB-kunnandet breddats även bland människor som inte har ADB som arbetsinstrument.

Andra inslag i utvecklingen har varit ett ökande intresse i massmedia för de mer dramatiska sårbarhetsinslagen. Som exempel på uppmärksammade inslag kan nämnas inndustrispionage i Sverige av utländsk makt, ett antal "hackers"- incidenter, som också hämtade inspiration från den amerikanska filmen War Games, problem med amerikansk exportlagstiftning, den s k containeraffären och andra besläktade incidenter. Ökad kunskap om de mera exotiska tekniska hoten som röjande signaler, RÖS och den elektromagnetiska pulsen, EMP har också något förändrat bilden. RÖS behandlas i avsnitt 5.12 medan EMP-problematiken behandlas i SÅRB:s rapport 1985:1 ADB i kris och krig. Till det ökade intresset för ADB-sårbarhetsfrågorna har säkert också SÅRB:s aktiviteter bidragit.

Sårbarheten har en strategisk, överordnad aspekt som är av stor betydelse för effektiviteten i verksamheten och som måste påverka systemutformningen. Detta gör sårbarhetsfrågan till en vital angelägenhet för varje verksamhet, som i väsentlig grad är ADB-beroende. Något av detta har SÅRB diskuterat i sin rapport 1985:4 "Systemkomplexitet och sårbarhet".

SÅRB konstaterar att man trots uppmärksammade presentationer och god press inte lyckats förankra säkerhetsfrågorna på de rätta belutsnivåerna.

SÅRB har ansett det lämpligt att i huvudsak hålla fast vid den beskrivning av sårbarhetsfaktorer och den indelning i arbetsområden som beredningen gjorde i handlingsplanen. Självfallet har förutsättningarna ändrats under de år som gått sedan planen las fram. Några projekt har tillkommit medan några har bortfallit därför att de mist sin aktualitet. Vilka projekt det är fråga om och omvärderingar som gjorts framgår av projektbeskrivningarna under avsnitt 5.

Emellertid kan man nu konstatera att det sedan SÅRK:s tid skett en förskjutning av fokus i sårbarhetsdebatten och i SÅRB:s arbete. Från de mera exotiska och kriminella problemen som terrorism och missbruk för politiska syften har det huvudsakliga intresset förskjutits mot det mera vardagliga och sådant som också har betydelse för effektiviteten i ADB-verksamheten. En sådan förskjutning av intresset kan synas naturlig. Vardaglig ordning och reda, god personalpolitik, utbildning etc utgör förutsättningar för att den mera avancerade brottsligheten skall kunna upptäckas och bekämpas framgångsrikt liksom för att verksamheten skall kunna hållas igång även om datorerna slås ut eller av andra skäl blir obrukbara.

3.3 Hur SÅRB arbetat

Av beredningens direktiv och historiken sådan den återges i denna slutrapport framgår klart statsmakternas önskemål att kommittén skulle bedriva sitt arbete så att de som ansvarar för databehandlingen i Sverige skulle bli mera medvetna om sina egna systems sårbarhet och även sätta sig in i eventuella beroendeförhållanden gentemot andra, externa eller interna system. Härigenom skulle vi utan lagstiftning och byråkrati få ett mera säkerhetsmedvetet och stryktåligt samhälle.

För att nå detta mål har SÅRB arbetat på ett sätt som är mindre vanligt för statliga kommittéer. SÅRB har sökt ett så brett samarbete som möjligt med näringslivet. Detta har skett genom en efter hand utökad näringslivsrepresentation i beredningen, genom att bedriva flera av sina projekt i samarbete med olika icke-statliga organ.

Som exempel kan nämnas utvecklingen av SBA som genomfördes i samarbete med Riksdataförbundet och som nästan helt finansierades av SAF, Industriförbundet, bankerna, försäkringsbolagen, datorleverantörerna, kommun- och landstingsförbunden, de affärsdrivande verken och ett antal stora statliga myndigheter. Till detta kom alla de personella resurser som företag och organisationer ställde upp med i utvecklingsarbetet. SÅRB svarade för initiativ och projektledning.

Kortvarianten "SBA-kompakt" utvecklades och finansierades i samarbete mellan SAF,Industriförbundet, Sveriges hantverks- och industriorganisation – Familjeföretagen, SHIO, Grossistförbundet, SÅRB och Riksdataförbundet.

Krypteringsprojektet, som resulterat i en "hjälpreda" om kryptering finansierades av statskontoret, Televerket, Ericsson Radio Systems, IBM, Volvo, Posten och Sparbankernas Datacentraler AB, SPADAB.

Ett par andra projekt har genomförts i samarbete med SIG/SEC, en ideell förening inom Svenska Samfundet för Informationsbehandling, SSI med huvudsakligen säkerhetsexperter som medlemmar.

Broschyren Läckande datorer – en information om RÖS (röjande signaler) som hittills gått ut i en upplaga på 14 000 exemplar har finansierats gemensamt av Brottsförebyggande Rådet (BRÅ) och SÅRB.

Skolöverstyrelsen har bekostat broschyren Den sårbara datorn, som distribuerats i mer än 10 000 exemplar bl a till alla landets högstadie- och gymnasieskolor.

De olika medverkande företagen och organisationerna har även ställt upp med personella resurser.

Utredningsresurser har vidare i stor utsträckning kunnat hämtas från statliga myndigheter, främst statskontoret och Televerket. Stat, kommun och näringsliv har också bidragit och medverkat i referensgrupper i de olika projekten. Genom denna arbetsform har arbetet kunnat bedrivas med endast blygsamma direkta resurstillskott från regeringen. Kostnaden för SÅRB:s verksamhet sedan beredningen tillkom 1981 har sålunda totalt uppgått till mindre än 4 miljoner kronor.

SÅRB har kontinuerligt, allteftersom de planerade projekten fullföljts givit offentlighet åt utredningsresultaten. I några fall har rapporter tryckts i mera påkostat utförande men normalt har en upplaga om några hundra

exemplar producerats av kanslihusets offsetcentral. Rapporterna har distribuerats dels enligt särskild sändlista till ett 50-tal statsmyndigheter och affärsverk, till kommuner, landsting och ett urval näringslivsorgan, dels till nyhetsbyråer, dagstidningar, datatidningar och ett urval specialtidningar. Rapporterna har vidare utan kostnad överlämnats till var och en som så begärt.

Av stor betydelse för att väcka det intresse för sårbarhetsfrågorna som är en förutsättning för att nå de mål som statsmakterna uppsatt för SÅRB är goda och täta relationer med massmedia. SÅRB har därför särskilt vårdat sig härom vilket synes ha uppskattats och medfört omfattande publicitet och bidragit till det avsevärt ökade intresset för säkerhetsfrågorna under de senare åren.

SÅRB har väckt internationell uppmärksamhet. Det förhållandet att Sverige var så tidigt ute med sårbarhetsdebatten genom SÅRK och SÅRB har gett oss en framträdande position utomlands. Sverige anses internationellt ligga långt framme på detta område. Denna position som vi bör se till att behålla kan vara till nytta vid tjänsteexport och vid försäljning av svenska produkter på data- och elektronikområdet.

Intresset för ADB-säkerhetsfrågorna har på senare år ökat i utlandet. I Norge tillsattes en statlig sårbarhetskommitté år 1982. På EG-kommissionens uppdrag har under senare år genomförts en sårbarhetsstudie i de fem största EG-länderna. USA, Canada, Japan och Kina har på olika sätt visat ett starkt intresse för sårbarhetsfrågorna och SÅRB:s verksamhet.

SBA-metoden har översatts till norska, finska och engelska. Intresse för en översättning finns även i Tyskland och Italien.

4 Rådgivning/information, remisser och initiativ

4.1 Rådgivning och information

De aktiviteter som hör hemma under den här rubriken är av två typer. Dels har information lämnats genom den rapportutgivning som ägt rum kontinuerligt under åren allteftersom beredningens olika projekt fullföljts, dels har beredningens ordförande och sekreterare varit efterfrågade och flitiga informatörer på seminarier, kurser m m i datorämnen där sårbarheten haft en plats. Vilka rapporter m m som getts ut under åren framgår av bilaga 2. Initial distribution har i allmänhet skett i ett par hundra exemplar till press, myndigheter, organisationer och närmast berörda företag. Eftersom rapporterna uppmärksammats i pressen har många efter hand hört av sig till SÅRB och beställt rapporter. Distribuerade upplagor har för olika produkter varierat mellan c 300 och 14 000 exemplar. På några håll, särskilt kan nämnas Kommundata, har SÅRB:s rapporter mångfaldigats – i några fall i tusentalet exemplar för att distribueras i samband med utbildning m m.

Framträdanden vid konferenser och seminarier har skett ett par gånger per vecka under årets mest aktiva månader. I några fall har det varit fråga om framträdanden i utlandet.

Andra informationsaktiviteter som i och för sig kunde varit intressanta och övervägts, t ex att utge ett periodiskt nyhetsblad eller konferenser i SÅRB:s egen regi har måst förkastas på grund av tids- och resursbrist.

För rådgivning utöver de här nämnda informationsaktiviteterna har inga resurser funnits.

4.2 Remisser

Enligt SÅRB:s direktiv var det en huvuduppgift för beredningen att fungera som remissinstans på sårbarhetsområdet. "Främst gäller detta vid investeringar i stora datasystem på den statliga sidan. Det är väsentligt att sårbarhetsfrågorna blir beaktade innan statsmakterna fattar beslut om stora eller eljest viktiga ADB-system."(Dir 1981:48)

Under årens lopp har till SÅRB remitterats 12 departementsremisser och ett 10-tal andra remisser från myndigheter och andra organ. De flesta av departementsremisserna har rört ärenden av annan och mera allmän art än de som särskilt avsågs i direktiven, exempelvis betänkandet (SOU 1983:52) Företagshemligheter och betänkandet (SOU 1984:69) Säker elförsörjning.

Endast ett ärende har enligt direktivens intentioner formellt remitterats till SÅRB – statskontorets rapport om basregister över företag och andra organisationer remitterades i september 1983 till SÅRB.

SÅRB skrev i mars 1982 till regeringen och erinrade om vad som uttalats i direktiven och hemställde om att sådana rutiner infördes att sårbarhetsprövning regelmässigt skulle komma till stånd vid större eller på andra sätt viktiga investeringar i ADB-system. SÅRB föreslog att sårbarhetsprövningen skulle anslutas till den särskilda handläggningsordning som tillämpas för investeringar i statliga ADB-system och framhöll betydelsen av att sårbarhetsprövningen sker på ett tidigt stadium i utvecklingen av ett informationssystem. Framställningen föranledde ingen åtgärd.

I augusti 1982 skickade SÅRB ett cirkulärbrev till ett 100-tal statliga myndigheter. I brevet nämns att SÅRB avsågs vara remissorgan i sårbarhetsfrågor och att myndigheter enligt SÅRB:s direktiv borde samråda med SÅRB i de frågor inom dataområdet som rör sårbarhet. SÅRB ville genom brevet fästa uppmärksamheten på dessa sina åligganden "i syfte att beredningen framdeles i större omfattning bereds möjlighet att yttra sig i här aktuella frågor". Brevet hade, som framgått ovan ingen effekt.

4.3 Initiativ

Utvecklingen sedan SÅRB tillkom har i några fall motiverat att SÅRB tagit initiativ i aktualiserade sårbarhetsfrågor. Ett par av dessa har nämnts bland projekten, ex Uppringda förbindelser om hackers-problemen och Läckande datorer om problemen med s k röjande signaler. Ett annat problem som föranlett ett initiativ från SÅRB:s sida rör postens system för transportplanering.

4.3.1 Postens transportstyrningssytem, PTS

SÅRB uppmärksammade i maj 1985 att Posten var i färd med att bygga upp en databas avsedd för transportplanering. SÅRB beskrev i en PM inledningsvis hur systemet avsågs fungera och angav då bl a följande:

Systemet kommer att omfatta mycket ingående och detaljerade uppgifter om det svenska landskapet. Databasen kommer att innehålla hela Sveriges karta i digitalform. Underlaget är för hela riket karta i skala 1:50 000 (i inre Norrland 1:100 000). För tätorter gäller begrepp som finns med i Åkarförbundets vägatlas och tätortsbebyggelse om minst 2x1km. Kartan innefattar bl a kustlinjer, öar, sjöar större än 1 km2, vattendrag, järnvägar, flygfält. Vidare ingår vägupplysningar såsom hela svenska vägnätet ned till körbar stig, vägbeläggning, framkomlighet, broars tillåtna fordonsvidd, tillåtna axeltryck, vägtunnlars frihöjd och bredd. Posten avser även tillföra information om husnummer, bebyggelsetyp, våningplan/lägenhet.

Postens avsikt är att marknadsföra informationen till transportföretag, försvaret, polis, brandkår m fl myndigheter och enskilda som har intresse av effektiv transportplanering, exempelvis för att optimalt bestämma den snabbaste och mest framkomliga förbindelsen mellan olika orter med hänsyn taget till transporternas art och omfattning.

Uppgifterna i databaserna är inhämtade från olika offentliga myndighetsregister. När dessa offentliga uppgifter sammanförs och kombineras i PTS gör den samlade

informationsmängden och de möjliga bearbetnings- och sammanställningsmöjligheterna PTS till ett system som är mycket känsligt med avseende på den nationella säkerheten. Enligt militära experter blir PTS ett utomordentligt underlag för fientligt sinnad makts planering av militära operationer och för insättande av s k diversionsenheter (terroristverksamhet). Detaljrikedomen och aktualiteten ger ett underlag för att följa upp och inrikta satellitspaning och agentverksamhet. Skillnaden mellan säkerhetsgranskat kartmaterial och andra databaser kan utpeka just detaljer av intresse för dessa makter.

SÅRB redogjorde därefter för det juridiska läget och konstaterade att PTS data visserligen är inhämtade från offentliga källor men ändå borde ha sekretessgranskats i vart fall enligt kartspridningslagen (1975:370). SÅRB påpekade att det kunde antas att även andra stora företag med verksamhet inom transportväsendet vore i färd med att installera liknande system. SÅRB avslutade promemorian med följande synpunkter

Utvecklingen av den automatiska databehandlingen medför en efter hand allt fullständigare och mera detaljerad kartläggning av samhället inom snart sagt alla områden. Särskild lagreglering av ADB-register finns endast i fråga om personregister (datalagen 1973:289). Det står således var och en fritt – myndigheter,företag och organisationer – att inrätta för totalförsvaret känsliga ADB-register utan prövning av försvarsmyndighet och utan att saken ens kommer till myndighets kännedom. Sekretesslagen är endast tillämplig på myndigheter. Som exemplet med PTS visar är lagen ändå otillräcklig även där den kan tillämpas.

– – – –

De tekniska skyddsanordningar som kan tillämpas för att skydda ADB-register, behörighetskontroller, loggning etc är ej tillförlitliga. Mot en målmedveten angripare, särskilt med de resurser som en fientlig utländsk makt förfogar över, finns inget effektivt skydd.

Enligt SÅRB:s mening kan man inte utan vidare godta en utveckling som innebär en stor risk för att ADB-system och databaser med innehåll och omfattning som hotar totalförsvaret inrättas, i vart fall utan ansvariga myndigheters kännedom. Utvecklingen inom området måste följas och bevakas mera målmedvetet och intensivt än som hittills kunnat ske av ett organ med goda kontakter och insyn i ADB-branschen inom såväl myndigheter som den enskilda sektorn. Den eventuella författningsreglering som kan visa sig nödvändig för att följa och kontrollera utvecklingen i berörda avseenden ligger utanför ramen för denna PM.

I juni 1985 insände SÅRB promemorian till regeringen i försvarsdepartementet. I följebrev anfördes bl a att "Beredningen finner utvecklingen alarmerande och vill förorda att snara åtgärder vidtas för att förbättra statsmakternas möjligheter till överblick och påverkan av utvecklingen".

ÖB har i andra sammanhang föreslagit åtgärder för att förbättra skyddet för försvarssekretessen i samband med ADB-register. Dels har ÖB pekat på vikten av att ÖB ges tillfälle att granska och avge synpunkter på dataregister som kan behöva omfattas av försvarssekretess. I syfte att stadfästa detta förhållande har ÖB föreslagit att föreskriften i 4 § säkerhetsskyddsförordningen (1981:421) utvidgas till att gälla krav på samråd med ÖB då myndighet upprättar dataregister om det inte är uppenbart att registret saknar betydelse från totalförsvarssynpunkt. Dels har ÖB rest krav på åtgärder i syfte att få till stånd en ordning så att statsmakterna får bättre

överblick över datoriseringen och möjlighet att ingripa för att skydda information då det anses påkallat.

I ett regeringsbeslut i oktober meddelade regeringen att ÖB:s förslag bereds inom regeringskansliet och avskriver SÅRB:s framställning om åtgärder eftersom syftet med SÅRB:s framställning har vunnits.

5 Projekt

SÅRB har valt att avrapportera och distribuera utredningsresultaten efterhand som de blivit färdiga. De utredningsrapporter och andra publikationer som SÅRB under årens lopp har gett ut nämns i bilaga 2.

De projektbeskrivningar som SÅRB gör i detta avsnitt har – i de fall projektresultaten redan rapporterats – begränsats till en kortfattad redogörelse för projektet och de synpunkter och slutsatser som projektet lett fram till. I några fall har projekt avslutats helt nyligen och varit av den karaktär att de inte bedömts motivera en separat avrapportering. I dessa fall avrapporteras projektet i sin helhet i det följande.

SÅRB har i stort sett kunnat följa den planering som gjordes redan i handlingsplanen. Emellertid har utvecklingen sedan 1981 medfört att något planerat projekt mist sin aktualitet medan andra projekt, som inte var aktuella 1981, genom den utveckling som skett blivit intressanta och kommit att kräva insatser. Vilka det är fråga om framgår under respektive projektredogörelse.

Ordningsföljden mellan de olika avsnitten i kapitel 5 följer i huvudsak dispositionen i handlingsplanen.

5.1 Sårbarhetsanalys – SBA

5.1.1 Mål och utformning

SÅRB behandlade i handlingsplanen från 1981 de olika arbetsområden som beredningen ansåg att man borde ägna sig åt. Under rubriken "Metod för sårbarhetsprövning" anfördes följande.

SÅRB skall verka 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. Detta förutsätter dels att SÅRB kan öka medvetenheten hos främst berörda beslutsfattare men även hos ADB-specialister och användare av ADB-system, dels att SÅRB kan ge konkreta och användbara råd.

En annan av SÅRB:s huvudaktiviteter var att fungera som remissinstans på sårbarhetsområdet främst när det gäller investeringar i stora statliga datasystem samt att fungera som samrådsorgan när det gäller beredning av frågor inom dataområdet som rör säkerhet. För att SÅRB skall kunna genomföra detta krävs ett strukturerat och metodiskt angreppssätt.

Inom SÅRB:s ansvarsområde faller naturligt även ett ansvar för att främja

utbildning inom säkerhets- och sårbarhetsområdet, på ett sådant sätt att samhällets sårbarhet minskar. För att kunna genomföra utbildning krävs bl a en metod, som enkelt kan läras ut.

SÅRB skall dessutom lägga grunden till en fortlöpande bevakning av sårbarhetsområdet. Ett sådant arbete förutsätter att det finns en metod som möjliggör att sårbarhetsproblematiken kan angripas på ett strukturerat, metodiskt och praktiskt sätt.

En viktig uppgift för SÅRB var också att skapa en metod som uppfyllde vissa i handlingsplanen angivna mål:

Det enskilda företaget/myndigheten skall självständigt kunna pröva sin egen sårbarhet och beroende av externa system.

Det enskilda företaget/myndigheten skall självständigt kunna bedöma sina egna systems sårbarhet och deras betydelse för externa systems säkerhet.

Metoden skall utformas på ett sådant sätt att den förutsätter ett konkret och lättfattligt arbetssätt och att utbildningen i metodens användning kan ske med små resurser.

5.1.2 Utvecklingsarbete

SÅRB påbörjade i början av 1982 arbetet med att utveckla en metod för sårbarhetsprövning som kunde uppfylla de nämnda kraven. I en av de skrifter som utvecklingsarbetet resulterade i, "SBA Information" berättas "historien om SBA". Där sägs bl a

I SÅRB:s handlingsplan återfinns projektets metod för sårbarhetsprövning, eller sårbarhetsanalys (SBA) som det senare kom att heta. Uppgiften gick i korthet ut på att utveckla en enkel och praktisk metod, möjlig att använda av både företag och offentliga myndigheter. Målet var tvåfaldigt:

- SBA-metoden skulle resultera i säkrare datasystem hos företag och myndigheter.
- Genom bättre säkerhet hos samhällets stora, viktiga system skulle samhällets totala sårbarhet minska. SBA-metoden skulle helt enkelt bli ett steg mot ett robustare samhälle.

Redan från början stod det klart att SBA-metodens utveckling måste bli ett samarbetsprojekt om kraven på hög ambitionsnivå skulle kunna uppnås. Kontakt togs med Riksdataförbundet (RDF) som ställde upp som medansvarig i ett samarbetsprojekt, där företag, näringslivsorganisationer samt offentliga myndigheter ställde upp med ekonomiska och personella resurser. Det senare inte minst viktigt eftersom en metodutveckling av detta slag måste växa fram i samspel mellan kompetens och praktiska erfarenheter från skilda områden. Till projektet knöts ett stort antal medarbetare med kunskaper om praktiskt säkerhetsarbete, riskvärdering, revision m m, och med olika erfarenhetsbakgrund – små och stora industriföretag, bank- och försäkringsväsende, statliga och kommunala myndigheter.

SBA-metoden blev genom den gemensamma satsningen ett unikt projekt. Stat, kommuner och näringsliv har här tillsammans genomfört ett projekt i det klart uttalade syftet: att väcka till medvetande om samhällets ADB-beroende och att angripa den sårbarhet som följer därav.

Utvecklingsarbetet, som finansierades gemensamt av staten, kommuner, landsting och näringslivet, kunde slutföras under 1983 och avslutades med en presskonferens i september 1983 vid vilken försvarsministern, civilministern och Industriförbundets ordförande medverkade. SBA-metoden lanserades vidare genom informationskonferenser i Riksdataförbundets regi på flera platser i landet och genom en brevkampanj där ett informationsmaterial om SBA utsändes till ca 10 000 chefspersoner i statliga och kommunala myndigheter, i företag och organisationer. Lanseringen har följts upp genom ett flertal konferenser och seminarier.

5.1.3 Material och marknadsföring

SBA-metoden består av ett antal olika delar, som kan användas – var för sig eller i kombination med varandra – på det sätt som är lämpligt med hänsyn till den användande organisationens storlek och verksamhet samt tidigare erfarenhet av ADB-säkerhetsarbete. De olika delarna är följande:

SBA Start. Verkställande ledningens underlag för grov bedömning av verksamhetens sårbarhet med avseende på datoriserad informationsbehandling.
SBA Beroende. En metod att översiktligt analysera och dokumentera en verksamhets beroende av datoriserade informationssystem.
SBA System. En metod att översiktligt bedöma ett eller flera datoriserade informationssystems inverkan på verksamhetens totala sårbarhet.
SBA Scenario. En metod för att på kort tid bedöma en ADB-verksamhets – eller ett enskilt systems – sårbarhet och ge underlag till en handlingsplan för att höja säkerheten.
SBA Plan. Olika sätt att dokumentera handlingsplaner för att minska ADB-verksamhetens sårbarhet.
SBA Rapport. Olika sätt att inom en ADB-verksamhet löpande följa den relativa sårbarhetsnivåns förändring.
SBA Projekt. En metod att bedöma ett ADB-projekts möjlighet att nå sitt mål i rätt tid, till rätt kostnad och med rätt kvalitet.
SBA Utveckling. Ett konkret förslag till hur kontroll- och säkerhetsanalys kan genomföras och dokumenteras vid utveckling av ADB-system.
SBA Nyckelpersonal. En metod för analys och dokumentation av nyckelfunktioner inom datordrift.
SBA Revision. Information om externa och interna revisorers medverkan vid användning av SBA-metoden.

Sedermera har tillkommit **SBA Kompakt,** avsedd att användas av mindre företag och organisationer.

De olika delarna är upptryckta i separata häften. Dessa marknadsförs, liksom tillhörande handledningsmaterial, video m m av Utbildningsproduktion AB.

Under 1985 har tillkommit **SBA Risk,** som är en datoriserad riskbedömningsmodell utvecklad på privat initiativ.

5.1.4 Utvärdering

SBA-metoden har hittills prövats endast under 2 års tid, vilket är för kort för säkra slutsatser om metodens värde. Några försök har emellertid gjorts att värdera metoden.

Konsultföretaget Infosec Prosab AB vars ledning f ö medverkade i metodens utveckling gjorde i början av 1985 en serie intervjuer om SBA-metodens användning. Antalet intervjuade uppgick till totalt 133 myndigheter och företag. De allra flesta (110) var positiva till metoden efter att ha prövat åtminstone någon del av den. Endast en dryg tredjedel hade emellertid faktiskt använt metoden eller någon del av den på det avsedda sättet. De viktigaste skälen till att metoden ej kommit till bredare användning ens hos dem som alltså köpt materialet uppgavs vara tidsbrist och bristande stöd från verksamhetsledningen.

Inom Riksrevisionsverket, RRV pågår ett projekt som syftar till att granska statsmyndigheternas arbete med ADB-säkerhet. En förstudie påbörjades i november 1984 och avslutades med en rapport daterad juni 1985.

Statskontoret har i februari 1985 fått i uppdrag av regeringen att bl a undersöka vilka effekter mera omfattande störningar i den civila statsförvaltningens ADB-verksamhet i fredstid kan få för myndigheterna och samhället i stort. Regeringen uppdrog åt statskontoret att samarbeta med bl a RRV och SÅRB.

Inom ramen för det nämnda samarbetet beslutade RRV, statskontoret och SÅRB att inledningsvis genom en enkät inhämta uppgifter från myndigheterna för att översiktligt få belyst hur myndigheterna arbetar med frågor om ADB-säkerhet och myndigheternas bedömning av störningars effekter. Enkäten omfattade 48 frågor varav de sista 10 avsåg SBA och skulle besvaras endast av dem som använt SBA-metoden.

Enkäten utsändes till 160 myndigheter varav 120 inkom med svar. Endast 13 av dessa hade besvarat SBA-frågorna. Svaren är kortfattade och tillför ingen annan information av värde än att myndigheternas entusiasm för metoden förefallar svalare än hos dem som besvarade Infosec Prosabs frågor. En majoritet ansåg att metoden var bra men kunde förbättras *eller* att metoden var dålig.

I RRV:s rapport från förstudien "Myndigheters åtgärder för ADB-säkerhet – förstudie 1985-06-14" påpekas att det saknas riktlinjer för myndigheternas arbete med dessa frågor.

Efter en genomgång av de regler som finns beträffande ADB-säkerhet i bl a tryckfrihetsförordningen, sekretesslagen, allmänna arkivstadgan etc konstaterar RRV att "det saknas en enhetlig operationell och väl avvägd reglering för att styra och ge stöd åt arbetet med ADB-säkerhet."

Det framgår vidare av studien att det endast är någon enstaka myndighet som gjort någon systematisk sårbarhetsanalys. Som en följd härav saknar många myndigheter också en genomtänkt plan för hur de skall bedriva sin verksamhet om de drabbas av mer eller mindre allvarliga avbrott i datordriften.

RRV avslutar förstudien med ett förslag till huvudstudie vars resultat kommer att föreligga i början av 1986.

Erfarenheterna av SBA-användningen är bättre inom kommun- och landstingssektorn. Metoden har med goda resultat kommit till användning i större utsträckning än i staten. Man har även påbörjat ett projekt för att ta fram riktlinjer för hur den sårbarhet som påvisats genom analysen skall åtgärdas, särskilt i fråga om organisation och ansvarsfördelning.

5.1.5 SÅRB:s enkät

Det intressanta i detta sammanhang är egentligen inte att utreda hur bra eller dåligt SBA är för sitt ändamål utan snarare att ta reda på hur och i vilka avseenden metoden kan bli bättre. SÅRB har därför i syfte att komplettera annat erfarenhetsmaterial *dels* medverkat i ett erfarenhetsseminarium arrangerat av Riksdataförbundet *dels* gjort en begränsad enkät riktad till 15 utvalda personer som inom företag och myndigheter genomfört och ansvarat för sårbarhetsanalyser med användning av SBA-metoden.

Erfarenheterna kan sammanfattas enligt följande

- Metoden har prövats och visat sig användbar inte bara för administrativa utan även för processdatasystem och CAD/CAM-system. Metoden har också med framgång använts för sårbarhetsanalyser av annan teknisk utrustning än datorer.
- Metoden är svår att använda utan specialisthjälp, som behövs åtminstone för att komma över igångsättningsmotståndet. Specialisthjälp är också värdefull därför att man ofta är "hemmablind".
- Metoden omfattar alltför många delar – det kostar tid och pengar att pröva sig igenom alla. Det hade räckt med ett par, tre metoddelar. Till slut fastnar de flesta för att använda särskilt SBA Scenario som man då kan anpassa efter det egna behovet. Det är bra.
- Metoden bör kompletteras med en exempelsamling eller ett genomgående praktikfall till hjälp för dem som skall göra sin första sårbarhetsanalys. Metoden bör kompletteras med hur man säkerhetsklassificerar data och information.
- Det saknas stöd för hur man skall använda resultatet av en genomförd sårbarhetsanalys.
- Det behövs bättre handledning, som belyser syftet med och sambandet mellan olika SBA-delar.
- Metoden har avsevärt ökat intresset för och kunskapen om sårbarheten. Dock inte i lika hög grad hos företags-/myndighetsledningen. "Missionsarbetet har alltför mycket riktats mot de redan frälsta", som någon av de 15 uttryckte saken.
- Metoden har underlättat säkerhetsarbetet och lett till att säkerhetshöjande åtgärder vidtagits.

Har SÅRBs mål med SBA, så som de uttrycktes i handlingsplanen uppnåtts? Medvetenheten har odiskutabelt ökats. SÅRB har genom att hänvisa till SBA kunnat fullfölja vad som krävdes i fråga om konkret rådgivning. Däremot har SBA inte kommit till användning som mall eller mätmetod för att SÅRB strukturerat och metodiskt skulle kunna ta ställning till remisser beträffande stora statliga datasystem etc. Skälet härtill är helt enkelt att SÅRB aldrig fått sådana remisser.

SBA har vidare visat sig vara användbar och pedagogisk i utbildningssammanhang.

SBA utgör en god grund att bygga vidare på i den fortlöpande utvecklingen av metoder för sårbarhetsanalys.

5.1.6 Slutsatser och rekommendationer

- SBA bör modifieras och kanske förenklas med ledning av de erfarenheter av metodens användning som vi nu har.
- De statsmyndigheter som är av särskild betydelse för totalförsvaret bör enligt SÅRB:s mening åläggas att *dels* analysera sårbarheten i sin datorbaserade verksamhet med SBA eller annan likvärdig metod, *dels* utarbeta plan för hur myndigheten skall fullgöra sina uppgifter vid bortfall av datorkraften.

5.2 Utlandsberoendet

Frågan om utlandsberoendet som en sårbarhetsfaktor behandlades relativt utförligt redan av SÅRK. I handlingsplanen anfördes att beroendet ökat sedan SÅRK skrev sitt betänkande.

I september 1982 tillkallade regeringen en särskild utredare för att "utarbeta ett brett, inledande material om dataflödena över Sveriges gränser och dessa flödens betydelse". Syftet med utredningen var att snabbt få fram ett faktamaterial om dataflödenas omfattning och karaktär samt att få belyst de växande dataflödenas betydelse för individer, företag och samhälle. Utredningen framlade i november 1984 en rapport med namnet "Sveriges datakommunikationer med utlandet – en inventering", Ds C 1984:4A.

Svenska industriföretags sårbarhet och interna anpassningsförmåga när det gäller att klara olika avspärrningssituationer behandlas i en forskningsrapport nr 15 1982 från Industriens utredningsinstitut, IUI "Industriföretagets sårbarhet".

En annan aspekt av utlandsberoendet behandlades som en 3-betygsuppsats vid företagsekonomiska institutionen, Uppsala universitet i september 1984. Uppsatsen har titeln "Svenska företags beroende av licensbelagd amerikansk elektronik".

Statskontoret har biträtt SÅRB med utredningsresurser och i några PM belyst utlandsberoendet i fråga om programvara, utlandsbearbetningar samt fjärrservice och underhåll.

5.2.1 Kategorier

Utlandsberoendet på datorområdet kan avse följande kategorier:

- Mikroelektronik (chips), som kan betraktas som en råvara som numera ingår i en mycket stor del av de produkter som verkstads- inklusive datorindustrien producerar.
- Datorer inklusive periferiutrustning, reservdelar, komponenter.
- Programvara.
- Personal och kompetens.

- Databaser i utlandet, dels databaser för informationssökning, dels databaser som används av företag och andra organisationer i deras operativa verksamhet.

5.2.2 Hotbilder

Hur allvarliga effekter vårt utlandsberoende får är naturligtvis beroende på arten och omfattningen av störningar i våra relationer med utlandet. För det aktuella ändamålet torde det räcka med att diskutera två kategorier av situationer. Den ena omfattar situationer i fred men med mer eller mindre allvarliga störningar i våra relationer med utlandet. Denna kategori av hot har under senare år fått ökande aktualitet bl a genom USA:s skärpning av exportkontrollen av högteknologi och då särskilt elektronikprodukter. Allvarligare varianter av den här hotkategorien är embargo, handelshinder av annat slag eller regelrätt handelskrig. Elektronikprodukternas karaktär av sofistikerat insatsmaterial som integreras i de mest skilda produkter kan göra det särskilt intressant att använda elektronik som medel för utpressning.

Åtgärder på handelsområdet kan vara attraktiva för en angripare även av andra skäl. Insatsen, hotet, kan exakt anpassas efter situationens allvar och sättas in mot den svaga punkten där små insatser kan få stora effekter. Ett exempel härpå kan vara det kontroversiella amerikanska förbudet mot leveranser till den nya gasledningen från Sovjetunionen till Västeuropa för något år sedan.

Den andra kategorien av hot utgörs av de extrema situationer där landet helt eller delvis är avskuret från kontakter med utlandet genom att krig råder i vår omvärld.

SÅRB har i projektet ADB i kris och krig avsnitt 5.9 arbetat med mera utvecklade hotbilder.

5.2.3 Mikroelektronik

ÖEF har oroats av det starka beroendet framför allt av amerikansk elektronik och den dåliga beredskapen mot importstörningar och avspärrning. ÖEF har därför inlett ett projekt som syftar till att genom olika åtgärder förbättra beredskapen. I ÖEF:s projekt ingår att inledningsvis identifiera de viktigaste samhällsfunktionerna, som alltså måste kunna försörjas med elektronik, att "sälja beredskapstanken", dvs göra elektronikanvändarna medvetna om behovet av beredskapsplanering, att kartlägga elektronikmarknaden och möjligheterna att påverka den i gynnsam riktning bl a genom standardisering och ekvivalentlistor. Man vill vidare undersöka möjligheterna att beredskapslagra elektronik. Regeringen har beviljat medel för de nämnda projekten.

Mot den här bakgrunden har SÅRB ansett det lämpligt att avstå ifrån att vidare utreda frågor om utlandsberoendet i fråga om mikroelektronik.

5.2.4 Datorer, reservdelar m m

Om man till en början väljer att behandla datorer och kompletta datorsystem kan det finnas anledning att först se på vad som brukar kallas för

spetsteknologien, det senaste på datorområdet – ofta utrustning av typ "dual use". Dual use avser utrustning som är särskilt lämpad att använda både för krigiska och fredliga ändamål. Sådana datorer kan självfallet komma att utnyttjas i samband med handelsstörningar och påtryckningar i fred. Våra möjligheter att minska sårbarheten är i detta avseende mycket små. Den amerikanska exportlagstiftningen har vi lika små möjligheter att påverka som vädret eller andra "acts of God". Att finna substitut eller alternativ till den här typen av utrustning låter sig inte heller göra. De svenska myndigheterna och företagen är emellertid väl medvetna om situationen och kravet att följa de spelregler som amerikanerna fastställt. Regeringen har i syfte att minska riskerna för problem uppdragit åt försvarets materielverk att i samråd med Industriförbundet utarbeta och administrera ett arrangemang för förstärkt sekretesskydd av dual-use-teknologi.

I den andra hotkategorien – krig i vår omvärld, torde vi under den aktuella tidsperioden under alla förhållanden vara tvungna att leva med den spetsteknologiutrustning vi har vid krigsutbrottet. Förutsättningen är dock att vi skyddar de dyrbara datorerna, alternativt beredskapslagrar reservdatorer, så att vi inte blir beroende av ersättningsleveranser t.ex för den krigsindustri vi under dessa förhållanden kan hålla igång.

Då det gäller andra datorer än de allra mest avancerade är förhållandena något annorlunda. Smådatorer tillverkas i många länder inklusive vårt eget land och kan knappast utnyttjas i en handelskonflikt. Stordatorer kan däremot åtminstone teoretiskt, komma att användas som brickor i sådana konflikter. Ändå finns det flera skäl som talar emot detta. Det finns många konkurrerande fabrikat och flera konkurrentländer även om USA dominerar stort även här. Ett annat kanske inte helt betydelselöst förhållande är att branschen domineras av mycket stora, multinationella företag. Dessa har byggt upp sin världsomspännande verksamhet på en internationell arbetsfördelning i vad avser både forskning, utveckling och produktion. I den mån man tillmäter dessa giganter någon makt och något inflytande över sina hemländers regeringar – och många är ju bekymrade över de multinationella företagens inflytande – måste man anta att de utgör en kraft som verkar *för* fri handel och konkurrens och *mot* handelshinder. Det är alltså svårt att tänka sig begränsade handelskonflikter där konventionella stordatorer utnyttjas som medel att framtvinga eftergifter. I en allvarligare situation kan naturligtvis stordatorer dras in men då sannolikt endast som en produkttyp bland flera andra och i ett läge där handelskonflikten utgör ett förstadium till en väpnad konflikt.

I den tänkta krissituationen måste man utgå från att all tillförsel till landet av stordatorer stoppas. Ändå är det rimligt att göra den bedömningen att vi utan oöverstigliga svårigheter skall klara en tvåårig avstängning särskilt med tanke på att behovet av datorkraft radikalt minskar i ett sådant läge.

Situationen ter sig annorlunda för tillbehör och reservdelar till datorer men sannolikt klarar vi oss i två år utan tillförsel av nya, kompletta datorsystem. Större delen av reservdelsförsörjningen liksom service och reparation av datorer ombesörjs av leverantörsföretagen. En ökande andel, särskilt av vissa produktsegment, svarar dock s k tredjepartsföretag för. Dessa är företag som marknadsför service, reparationer etc utan att som leverantörer ha särskilda intressen i den utrustning man tar hand om. Tredjepartsmark-

naden omfattar f n 10-25% av den totala servicemarknaden. Den omfattar huvudsakligen terminaler och smådatorer medan stordatorservicen nästan helt sköts av leverantörsföretagen.

Liksom inom andra branscher eftersträvar även denna att hålla så små reservdelslager som möjligt. Lagret – eller åtminstone större delen av det – befinner sig så att säga på väg.

IBM uppger att man lagerhåller reservdelar dels centralt för landet, dels i ett antal sekundärlager ute i landet. Härigenom skall man klara en utlovad leveransberedskap på två timmar. 95% av reservdelarna levereras ifrån dessa lager, resten måste hämtas från ett Europalager i Frankrike och kan då levereras inom 24 timmar.

Leveranser från Europalagret till de dator-optimerade svenska lagren sker med en leveranstid på 8 veckor. Beställningspunkten ligger alltså 8 veckor före slut. Man anser att man med större sparsamhet och försiktighet skall klara 4-6 månaders avstängning utan allvarliga driftproblem. Om man därtill får möjlighet att utnyttja en del av maskinparken som reservdelsdepåer tror man att det skall gå att hålla igång 2-4 år.

Över huvudtaget förekommer reparationsservice, s k korrektiv och preventiv service endast mycket sparsamt. Serviceingenjörerna ägnar sig huvudsakligen åt installationsarbete och s k systems assurance, som innebär kontroll av att installerad utrustning uppfyller garanterade specifikationer.

Man uppger också hos IBM att moderna datorer är så kompakt konstruerade att egentliga reparationer inte längre förekommer utan att felservicen huvudsakligen består i att byta ut separata, defekta delar, t ex kretskort. De felaktiga kretskorten ersätts med nya.

De programprodukter som ingår i datorleveransen sköts på motsvarande sätt. Produkterna är uppbyggda modulärt och utbyte sker av hela moduler.

Det största av de företag som är verksamma inom tredjepartsmarknaden är TELUB AB som numera är ett dotterbolag till det helt statligt ägda FFV ELEKTRONIK AB. TELUB uppger att man har 43% av tredjepartsmarknaden i Sverige och dessutom bedriver verksamhet i utlandet, särskilt i våra grannländer.

Tredjepartsservice underlättas av samarbete med leverantörsföretagen. Dessa måste ju bl a tillhandahålla dokumentation över den utrustning som skall skötas av tredjepartsföretaget. Emellertid är det ju så att datorleverantörerna har en inställning eller policy som i flera avseenden avviker från den som en kvalificerad och stark köpare av produkterna naturligen har. Det ligger t ex inte primärt i leverantörernas intresse att arbeta för en standardisering av sin marknads produktutbud i bl a de avseenden som har betydelse för servicevänligheten. Det kan ligga mera naturligt till för en leverantör att tillämpa slit-och-släng i fråga om reservdelar till datorer ungefär så som IBM beskrev sin service, dvs byta ut hela kort/moduler och ersätta med nya. För en dominerande leverantör som IBM kan det vara mest gynnsamt att utestänga tredjepartsservice genom att utnyttja egenutvecklad och IBM-specifik elektronik. Underhållsmässigheten, som rimligtvis är en betydelsefull faktor för att minska sårbarheten, prioriteras inte. De här nämnda förhållandena hindrar inte att tredjepartservice förekommer även

beträffande IBM:s produkter, t ex av dess PC i Sverige och även av stordatorer ute i Europa. Än mera utbredd är sådan service i fråga om de mindre dominerande stordatorföretagen.

Tredjepartsföretagen har å andra sidan prioriteringar och egenskaper som är positiva från beredskapssynpunkt. Man reparerar och rekonditionerar i stället för att kasta. Man bygger upp en inhemsk, kvalificerad servicekompetens på komponentnivå, man har erfarenhet av att tekniskt uppdatera utrustning, att "slakta" uttjänt utrustning för att få tillgång till delar, etc. Man arbetar helst med utrustning uppbyggd av standardkomponenter och är bekymrad över den ökande användningen av custom design-kretsar och sådan utrustning som ställer så speciella krav på reparationsmiljön att de måste skickas utomlands för reparation. Ett exempel på det sistnämnda är s k Winchesterminnen.

SÅRB:s undersökningar har visat att det inte finns anledning befara att brist på reservdelar och tillbehör skulle behöva uppstå i något av de skisserade scenarierna. Denna slutsats bygger dock på förutsättningen att vi vidtar beredskapshöjande åtgärder av den art som vi återkommer till avslutningsvis i detta avsnitt.

5.2.5 Programvara

För det här aktuella ändamålet är det lämpligt att granska två skilda typer av programvara. Dessa är tillämpningsprogram och systemprogram.

De amerikanska reglerna för exportkontroll gäller även teknologi eller Technical Data. Med sådana "tekniska data" avses bl a viss programvara för datorer. Det förekommer att mjukvara förses med inbyggda s k logiska bomber som utlöses och fördärvar programmet den dag som detta t ex inte får sin påbjudna auktoriserade service, kanske därför att det utgör en piratkopia. I de fall det är fråga om utländsk programvara kan detta förfarande naturligtvis medföra särskilda risker.

Den inledningsvis nämnda utredningen om Sveriges datakommunikationer med utlandet har kartlagt vårt lands beroende i dessa avseenden. När det gäller tillämpningsprogram är vårt beroende totalt sett mindre vilket dock inte hindrar att det kan finnas ett eller annat område där vårt beroende är stort och absolut. Exempel härpå finns. Det kan här finnas anledning till fortsatt noggrann bevakning för att förhindra att för vårt land viktiga funktioner blir beroende av utländska programleverantörer.

Systemprogramvara och liknande med datorutrustning mer eller mindre integrerad programvara har från sårbarhets- och beredskapssynpunkt samma egenskaper som den hårdvara med vilken den samverkar. Även här kan, för att nämna ett exempel, tredjepartservice komma in i bilden och krav ställas på att leverantören tillhandahåller utbildning, dokumentation m m som underlättar för andra än leverantören att sköta service och underhåll.

F ö torde det vara så att användarna inte är så kritiskt beroende av att ständigt och omedelbart få tillgång till den senaste versionen av t ex ett operativsystem. Det går faktiskt att under ganska lång tid leva vidare med den hård- och mjukvarukonfiguration som man råkar ha vid ett avspärrningstillfälle.

5.2.6 Personal och kompetens

Det har i debatten förekommit farhågor för att leverantörsföretagens tillämpning av fjärrdiagnos och fjärrservice skulle minska yrkesskickligheten hos serviceteknikerna och därmed öka vår sårbarhet vid avspärrning – särskilt förstås om fjärrdiagnoscentra eller motsvarande är förlagda utomlands. IBM:s Remote Support Facility, RSF består i huvudsak av en databas innehållande uppgifter om tidigare inträffade fel och problem och hur de avhjälpts. Dessutom används systemet för brevlådekommunikation mellan servicetekniker. Databasen finns i USA, Japan, Holland och Storbritannien. Man uppger från svenska IBM att systemet ej medför någon uttunning av kompetenser – IBMs servicetekniker får en mycket gedigen utbildning som bl a innefattar tjänstgöring vid de utlandscentra där servicekompetensen är koncentrerad. Emellertid har det framkommit även andra synpunkter som ger visst belägg för farhågorna. Fjärrdiagnosen tar bort incitamentet att själv leta fel – en konst som man då så småningom glömmer bort. I kombination med den slit-och-slängmetod som tillämpas är det viss risk att servicekompetens går förlorad.

Desto viktigare är den kompetens som byggs upp hos tredjepartsföretagen. Man reparerar utrustning på komponentnivå och har ibland men inte alltid tillgång till respektive leverantörsföretags fjärrservicesystem. I de fall man ej får utnyttja den bygger man upp sin egen erfarenhetsdatabas.

I detta sammanhang finns anledning peka på risken för obehörig åtkomst av data i samband med fjärrdiagnostik. Denna kan nämligen innebära eller ställa krav på att innehåll i minnesmedium töms och analyseras för att eventuella fel skall kunna hittas. Vissa minnesmedia, t ex Winchesterminnen är så konstruerade att de vid fel måste skickas till särskilda service-centra utomlands för analys och reparation.

Handelshinder har när det gäller våra servicemöjligheter inte någon relevans. Däremot skulle en avspärrningssituation med eventuella beredskapsinkallelser ha betydelse. Det är viktigt att tillse att servicepersonal placeras i eller får kvarbli i befattningar där de behövs för att hålla datorverksamheten i gång. För den reducerade databehandling som statsmakterna prioriterar under beredskap och krig torde våra serviceresurser under sådana förhållanden räcka väl till.

5.2.7 Databaser i utlandet

Grovt indelat kan man urskilja dels databaser som används för informationssökning, dels operativt använda databaser i t ex multinationella företag. Utredningen om Sveriges datakommunikationer med utlandet ger inget stöd för farhågorna att databaser skulle utgöra en kritisk sårbarhetsfaktor. Naturligtvis har t ex våra universitet och forskningsinstitutioner mycket stor nytta av databaserna för informationssökning och är i sitt arbete beroende av att kunna utnyttja dem. Men från totalförsvarssynpunkt är det ointressant om vi under begränsad tid avstängs från dessa databaser. Däremot kan det finnas anledning uppmärksamma risken för att svenska, multinationella företag som arbetar inom områden av betydelse för totalförsvaret för sin verksamhet i Sverige gör sig beroende av databaser hos sina utländska filialer.

5.2.8 Slutsatser och rekommendationer

Allmänt sett har Sverige bl a genom teknikutvecklingen utvecklats till ett alltmera sofistikerat och integrerat samhälle där det blir allt svårare att förutsäga vilka störningar som kan inträffa och vilka konsekvenserna av dessa kan bli. Det kan t ex knappast begäras att det enskilda företaget skall kunna rätt inse sin egen plats i och betydelse för totalförsvaret. Det är en specialistuppgift att kontinuerligt följa utvecklingen och vidmakthålla överblicken över vad som sker inom informationsbehandlingen så att det blir möjligt att ingripa i de fall utvecklingen hotar viktiga totalförsvarsintressen.

Vid sidan om denna generella bevakningsuppgift finns ett antal mera specifika åtgärder ägnade att minska utlandsberoendet, t ex följande:

- Utreda vilka system/datorer som är av sådan betydelse för totalförsvaret att de måste hållas i drift under kriser och krig respektive vilka system/datorer som vi kan klara oss utan och som vi i en krissituation kan utnyttja som reservdelsdepåer. Detta är den aktivitet som ÖEF planerar som ett led i sin mikroelektronikutredning men som också är av betydelse för en realistisk bedömning av resursbehovet i övrigt i en krissituation.
- Följa utvecklingen för att kunna förhindra att för vår beredskap och vårt totalförsvar viktiga funktioner blir beroende av utländska leverantörer av programvara till datorer.
- Stimulera till en ökad andel tredjepartservice genom att staten redan i avtal med leverantörer för in t ex följande klausul:
  Beställaren äger beställa underhållet av fristående underhållsleverantör. Leverantören är skyldig att samarbeta med av beställaren anlitad underhållsleverantör så att denne ges möjlighet att utföra underhållet på ett fackmannamässigt sätt. Härmed menas att underhållsleverantören erhåller tillgång till:
  - Reservdelar, utbytesenheter
  - Dokumentation
  - Utbildning
  - Teknisk support av såväl hård- som mjukvara
- Vid statlig upphandling ställa särskilda krav på underhållsplanering och underhållsmässighet.
- Statliga insatser för att utarbeta ekvivalenser och arbeta för utökad standard på komponent- och högre nivåer.
- Statliga insatser för att stimulera lagerhållning hos leverantör- och tredjepartserviceföretagen av komponenter i en omfattning som är motiverad av beredskapshänsyn men inte kommersiellt berättigad.
- Se över mobiliseringsplaneringen så att systemspecialister och servicetekniker i erforderlig omfattning kan fortsätta i sitt yrke även under beredskap och krig.

5.3 Utslagen datorkapacitet

5.3.1.Projektets bakgrund

SÅRB anger i sin handlingsplan att man *dels* hade för avsikt att kartlägga och följa upp de aktiviteter i fråga om reservkapacitet etc som var aktuella då, *dels* i ett särskilt projekt utreda de lösningsalternativ som finns vid olika typer av distribuering.

Att SÅRB valde att behandla just frågan om utslagen datorkapacitet, som endast utgör en begränsad del av det vida mera omfattande problemet med katastrofplanering berodde på att reservdatorfrågan särskilt nämndes i beredningens direktiv.

Under 80-talet har några uppmärksammade händelser ytterligare aktualiserat frågan om behovet av planering för reservdriftalternativ. Särskilt gäller detta det driftstopp som drabbade Värdepapperscentralen VPC AB och därmed aktiehandeln våren 1983. Stoppet berodde delvis på att reservdriftalternativ saknades. Vissa andra produktionsstopp, t ex i SJ:s bokningssystem har också föranlett viss publicitet och även politisk aktivitet. Allvarliga driftstopp har också drabbat vissa mindre påpassade verksamheter än VPC och SJ och bl a därför ej kommit till allmänhetens kännedom.

Bankinspektionen gjorde under 1983 en relativt omfattande undersökning av VPC:s dataproblem, leveransförseningar m m i samband med driftstoppet. Många av erfarenheterna och slutsatserna har allmänt intresse. Vad som skrivs i bankinspektionens rapport om VPC-systemets sårbarhet och ADB-säkerheten i systemet återges därför i bilaga 3.I bilagan ingår också VPC:s redogörelse för de säkerhetsåtgärder VPC vidtagit under åren 1983-1985.

5.3.2 Praktisk katastrofplanering – val av reservdriftalternativ

SÅRB har inte sett det som sin uppgift att behandla frågor om hur enskilda företag eller branscher löst eller skall lösa sina reservdriftproblem och vilka faktiska möjligheter härtill som f n står till buds. SÅRB har i stället valt att mera generellt och principiellt behandla frågan. Detta har skett i en rapport "Praktisk katastrofplanering – val av reservdriftalternativ".

Rapporten, som under 1984 skrevs av en konsult på uppdrag av SÅRB, riktar sig till personer i företag och myndigheter, som ansvarar för drift och katastrofplanering. Rapporten syftar till att beskriva vilka olika alternativ till reservdrift som finns vid utslagen datorkapacitet, för- och nackdelar med de olika alternativen och vad som kan påverka valet av dem.

Konsulten skriver i sammanfattningen att valet av alternativ styrs bl a av följande faktorer:

- Den tid inom vilken produktionen måste vara igång efter katastrofhändelsen.
- Storleken på erforderliga maskinella resurser.
- Behovet av datakommunikation.
- Den lokala situationen, dvs vilka andra företag finns på orten med samma problem? Var finns närmaste gemensamma backup-central? Vilket maskinfabrikat är det fråga om?

- De ekonomiska förutsättningarna.
- Andelen unik utrustning.

Schematiskt, i tabellform kan alternativvalet se ut på följande sätt.

Kapacitetsbehov % av normal drift				
76 –	Backup-central	Backup-central	Reservlokal + avtal med annan	Reserv-lokal
51 – 75	Backup-central	Backup-central	Reservlokal + avtal med annan	Reserv-lokal
26 – 50	Backup-central	Backup-central alt lokal	Reservlokal alt avtal	Avtal med annan
0 – 25	Avtal med annan	Avtal med annan	Avtal med annan	Avtal med annan
	<1 dag	<1 vecka	<2 – 4 veckor	tillåten avbrotts-längd

5.3.3. Slutsatser och rekommendationer

Som rapporten klart visar måste valet av reservdriftalternativ föregås av katastrofplaneringens två viktiga delvis sammanhängande aktiviteter.

Den ena består i att planera den datorstödda verksamheten – produktion, administrativa rutiner, etc så att det är klarlagt hur verksamheten skall fungera i en nödsituation – med nödvändigt bibehållet datorstöd, med nedskärningar av servicen och delar av verksamheten respektive eliminering av icke oundgängligen nödvändiga verksamhetsgrenar. Sådan planering måste i första hand ske i samband med systemutformningen.

Den andra aktiviteten består av de säkerhetstekniska katastrofplaneringsaktiviteterna varav reservdriftplaneringen är en viktig del.

5.4. Personrelaterade faktorer

5.4.1 Planerade aktiviteter

SÅRB har i handlingsplanen tagit upp fyra personrelaterade projekt.

- Kartläggning och åtgärdsförslag för att belysa frågor om beroendet av nyckelpersoner i ADB-verksamheten.
- Bevaka och ta erforderliga initiativ i fråga om utbildning av ADB-personal.
- Försök att kartlägga databrottslighet.
- Kartläggning av frågan om arbetsmarknadskonflikter och initiativ till åtgärder att minska den sårbarhet som sådana konflikter kan förorsaka.

5.4.2 Nyckelpersoner

Statskontoret genomförde 1983 på uppdrag av SÅRB en kartläggning av problemen med beroendet av nyckelpersonal. Resultatet redovisades i en rapport "Nyckelpersonal inom datordrift" vars syfte är att identifiera några viktiga personalgrupper och ge förslag till åtgärder som begränsar beroendet av dessa. Rapporten inleds med en genomgång av de olika personalkategorierna, deras arbetsuppgifter och kunskaper och de risker som beroendet av dem medför.

På åtgärdsområdet lämnas förslag till en metod för analys och dokumentation av nyckelfunktioner inom en organisations dataverksamhet. Metoden ingår som en av modulerna i SBA-metoden, SBA Nyckelpersonal. Modulen syftar till att göra det möjligt för en organisation att självständigt analysera vilka nyckelfunktioner som finns inom skilda områden av en ADB-verksamhet, t ex inom systemutveckling, driftorganisation och användargrupper. Genom analysen kan konstateras i vilka funktioner som reserver saknas, alternativt om eventuell kompetensbrist kan bli ett hot mot säkerheten.

5.4.3 Utbildning

Det är allmänt omvittnat att god utbildning i ADB-säkerhet för all ADB-personal är en förutsättning för att få en säkerhetsmedveten organisation. SÅRB har emellertid valt att särskilt ta upp och behandla frågor om både allmän och specialistinriktad utbildning i ADB-säkerhet under rubriken 5.10 **Utbildning.**

SÅRB har funnit att frågor om ADB-personal och ADB-säkerhet inte fått den behandling som ämnet med hänsyn till sin betydelse förtjänar. SÅRB har därför i en rapport **"Personal och säkerhet"** tagit upp frågor om rekrytering, utbildning, arbetsmiljö och organisation av ADB-verksamhet. Utgångspunkten är att det är "mänskligt att fela". Det måste ställas höga krav på människor som anförtros kvalificerade ADB-arbetsuppgifter. "Men de måste också ställa höga krav på den organisation och det system i vilket de skall arbeta. Möjligheterna att göra fel skall elimineras så långt det är möjligt, bl a genom förebyggande kontroller. Feltoleransen måste vara hög. Frestelser att otillbörligt utnyttja sin kunskap skall elimineras etc. Arbetsmiljön skall bidra till den harmoni som är en förutsättning för ett moget, omdömesgillt och balanserat handlande."

I rapporten behandlas frågor om ledningsansvar, ADB-säkerhetsansvar och säkerhetspolicy, om organisationsprinciper, om rekrytering, personalpolitik, yrkesetik och hantering av brott mot säkerhetsbestämmelser. En utförlig redogörelse lämnas för personalkontrollbestämmelserna.

5.4.4 Databrott

Svårigheterna att kartlägga databrottsligheten är allmänt välkända och omvittnade. Det s k mörkertalet är stort, enligt vissa bedömare över 90%. Termen databrott är dessutom obestämd till sin innebörd. Det kan råda delade meningar om vad som skall rubriceras som databrott.

Även bortsett från de nämnda svårigheterna har SÅRB ansett att man bör avstå från att lägga ner arbete på att kartlägga databrottsligheten. *Dels* har nämligen Rikspolisstyrelsen, RPS och dess arbetsgrupp med uppgift att utarbeta riktlinjer för polisens åtgärder mot databrott gjort en kartläggning av vad man kallar datakriminalitet, *dels* har Artur Solarz vid Brottsförebyggande rådet, BRÅ publicerat en forskningsrapport om databrott där man bl a menar att endast en mindre del av dessa upptäcks och att benägenheten att anmäla sådana brott är mycket låg.

RPS rapport "Polisens åtgärder mot datakriminalitet" är daterad oktober 1984 medan forskningsrapporten från BRÅ är från april 1985. Genom dessa produkter har vi tillförts ett kvalificerat och relativt uttömmande material om databrott.

5.4.5 Arbetsmarknadskonflikter

Att behandla frågan om arbetsmarknadskonflikter som sårbarhetsfaktor bereder som lätt inses avsevärda svårigheter. Självklart åligger det den som ansvarar för databehandlingens driftsäkerhet att göra vad som är möjligt för att gardera sig mot arbetsmarknadskonflikter liksom mot varje annan "katastrof". Det speciella med arbetsmarknadskonflikter och det som skiljer dem från andra "katastrofhändelser" är emellertid att de inte slår blint. En eldsvåda kan uppstå helt oberoende av om man planerat för en sådan händelse medan en konflikt – t ex strejk – sätts in just mot de verksamheter där beredskapen är dålig och undviks mot dem där beredskapen är god.

5.4.6 Extremiströrelser

En särskilt allvarlig typ av konflikter är emellertid sådana som inspireras och initieras av extremiströrelser, som riktas mot verksamheter av betydelse för totalförsvaret och som syftar till att störa viktiga samhällsfunktioner. Mot sådana konflikter måste man självklart skydda sig. Förebyggande åtgärder, bl a omfattande noggrann rekrytering och personalkontroll har berörts under avsnitt 5.4.4. I övrigt måste man noggrant planera för åtgärder i en sådan situation liksom för varje annan katastrofartad händelse.

SÅRB har inte ansett att dessa frågor har sådan betydelse eller prioritet att beredningen velat särskilt utreda dem.

5.4.7 Slutsatser och rekommendationer

Frågor om beroendet av nyckelpersoner, om hur dataverksamheten skall organiseras och administreras för att minska sårbarheten är enligt SÅRB:s mening mycket viktiga och hittills otillräckligt behandlade och utredda. SÅRB har med sina rapporter påbörjat en diskussion om dessa frågor som emellertid bör fortsätta och utvecklas. Genom SBA Nyckelpersonal finns numera en metod för att analysera den egna sårbarheten. Men ifråga om åtgärder saknas ännu mycket.

Risken för störning av ADB-verksamhet av betydelse för totalförsvaret genom vilda strejker måste liksom andra katastrofhot och -risker mötas med planering.

5.5 ADB-systemens komplexitet

5.5.1 Bakgrund

I handlingsplanen förde SÅRB fram uppfattningen att ADB-systemens komplexitet är en allvarlig sårbarhetsfaktor och att detta problemområde skulle belysas. SÅRB har därför med stöd av en referensgrupp med medlemmar från universitet, staten och näringslivet studerat komplexitetsproblemen och givit ut en rapport **"Systemkomplexitet och sårbarhet".**

5.5.2 SÅRB:s rapport

I rapporten konstateras att samhällsutvecklingen i många avseenden och inte minst tekniska ökar i komplexitet och att man måste acceptera detta. Men det är också viktigt att vi blir medvetna om våra egna mänskliga begränsningar i fråga om möjligheterna att förstå och behärska komplexa system. Symptomen på att ett system överskridit gränsen för hanterlig komplexitet är att de som ansvarar för systemet inte längre känner att de överblickar eller kontrollerar det. Det är inte längre möjligt att göra en ändring i någon del av systemet och vara säker på vad ändringen medför för konsekvenser i andra delar. Integreringen mellan olika system bidrar till svårigheter att ändra i ett system eftersom ändringarna stundom får konsekvenser, svåra att överblicka, även i andra system. Följden blir att man inte vågar eller anser sig kunna ändra systemet samtidigt som det byggs på och växer genom integration med andra system och situationen därmed ytterligare förvärras.

Självklart kan man inte skydda ett system effektivt om man inte kontrollerar det och känner dess gränser.

SÅRB diskuterar i rapporten några metoder att begränsa eller komma till rätta med komplexitetsproblemet. Det kan vara fråga om att bryta ner systemet i hanterliga delar åtskilda genom entydigt definierade gränser (interface), att öka standardiseringsgraden, att förbättra och automatisera dokumentationen. Ytterst torde det emellertid vara nödvändigt att förändra den traditionella systemutvecklingsmetodiken – främst lämna det procedurorienterade betraktelsesättet som medför låsning till stora system-/programblock och övergå till databasorienterade system där data och information utgör den fasta grunden medan programmen blir snabbrörlig förbrukningsvara. I sådana system blir datakvaliteten en särskilt viktig fråga. Med datakvalitet avses dels objektiv felfrihet, dels också kvalitativa egenskaper som t ex aktualitet, noggrannhet, relevans. En utveckling i den här antydda riktningen som f ö är angelägen av flera andra skäl medför en flexibilitet som på sikt är en nödvändig förutsättning för en kontrollerad systemförvaltning och – förändring. Det går inte att förbise att det ofta är det regelverk, som ligger till grund för systemet som starkt bidrar till komplexiteten.

Det har på senare år framgått att komplexitetsproblemen inte är unika för ADB-systemen. Liknande problem drabbar andra tekniska system. Det har därför växt fram ett intresse och en visserligen än så länge begränsad debatt i fackpress om dessa problem.

5.5.3 Slutsatser och rekommendationer

En systemutvecklingsmodell som baseras på s k datakataloger och databaser ställer höga krav på datakvaliteten. Frågor om hur datakvaliteten kan mätas, utvecklas och vidmakthållas har inte uppmärksammats tillräckligt hittills. Att öka vår kompetens och kunskap i datakvalitetsfrågor är enligt SÅRB:s mening en viktig forskningsfråga.

Systemkomplexiteten och hur den skall kontrolleras är också ett ämne som förtjänar en bättre genomlysning av forskningskaraktär.

SÅRB förordar att dessa ämnen blir föremål för forskningsinsatser.

5.6 Datakommunikation

5.6.1 Bakgrund och syfte

Datakommunikationen har under de senaste åren ökat i omfattning i accelererande takt. Därmed har också vårt beroende av datakommunikation och vår sårbarhet ökat.

Medan sårbarhet och säkerhet i databehandlingen har uppmärksammats och diskuterats i många år har datakommunikationen som självständig sårbarhetsfaktor knappt berörts förrän de allra senaste åren.

Det är framför allt i två avseenden som datakommunikationerna är utsatta för hot och risker. Det ena är dataskyddet, d v s obehörig avlyssning och störning av trafiken, det andra är funktionsskyddet eller driftsäkerheten.

Televerket har i en skrift "Risk management i Televerket", November 1983 bl a tagit upp riskerna för avlyssning, teleterror och obehörig åtkomst av kunduppgifter och nämner.

Avlyssning kan ske illegalt genom olika former av påkoppling på annans ledning induktivt eller med hjälp av dolda mikrofoner. Det är sannolikt att en ny mycket avancerad generation av dylika hjälpmedel ("buggar") är i bruk för närvarande. Dessa är nästan omöjliga att upptäcka eftersom de kan appliceras i samband med telekommunikationssystemets uppbyggnad på platsen eller placeras i spridningsnätet. Polisen anser att en stor mängd avlyssningsanordningar av olika slag i dag finns i det svenska telenätet.

Televerket nämner också i rapporten att "tillträdesskyddet vid televerkets datacentraler, -hallar och -rum i vissa fall är begränsat till enkla former av låsning och observation från personalen. Ett obehörigt intrång i en obemannad datalokal kan medge tillgång till mycket omfattande och/eller betydelsefull information samt möjlighet att manipulera systemen".

SÅRB har bedömt det vara av särskilt intresse att belysa dessa frågor för information och vägledning för dem som planerar och konstruerar system. Den som hanterar sekretessbelagd information måste kunna bedöma avlyssningsrisken och den som i t ex en verkstadsproduktion är absolut beroende av en ostörd och avbrottsfri kommunikation måste få faktaunderlag för att planera den.

5.6.2 Televerkets information

För att genomföra projektet och kunna erbjuda den vägledning vid systembygge som nämnts har SÅRB fått hjälp av en referensgrupp. Eftersom sakkunskapen i dessa frågor naturligen finns samlad i Televerket har det visat sig vara mest praktiskt att verket svarar för ett genomförande av projektarbetet i samråd med och enligt anvisningar från SÅRB. Arbetet har av olika skäl försenats och det färdiga resultatet kan därför inte föreligga förrän i början av 1986. Televerket kommer då att publicera en skrift med följande innehåll.

I en första avdelning redogörs för föreliggande risker för avlyssning och störning. Dessa risker omfattar särskilt följande

Avlyssning/Avtappning
- □ Oavsiktlig vid fel
  - i handhavande
  - i tekniken
- □ Avsiktlig
  - internationellt
  - lokalt
  - i växelutrustning
  - vid mellanlagring
  - röjande signaler

Driftstörningar och skador
- □ Avsiktliga fysiska skador
  - luftledningar
  - jordkablar
  - kulvertar
  - telestationer
- □ Avsiktliga störningar
  - spärrande trafikgenerering
  - substitution av behörig trafik
  - falsk terminal
  - elektro-magnetisk puls EMP
- □ Oavsiktliga störningar
  - väder
  - grävskopor
  - felkopplingar
  - elavbrott

I skriftens andra del kommer Televerket att redogöra för driftsäkerhetsförhållandena i telenäten i huvudsak enligt följande

Driftsäkerhet i telenäten
- □ Begrepp och teorier
- □ Sambandet mellan driftsäkerhet och ekonomi
- □ Driftsäkerhetsplanering i Televerket
- □ Driftsäkerhetsresultat – erfarenheter

- Driftsäkerhetsanalyser i
  - DATEL
  - DATEX
  - DATAPAK etc.
- Företags-/Tilläggsservice för utökad driftsäkerhet

5.6.3 Uppringda datorer

Mot bakgrund av ett antal incidenter under de senaste åren då s k hackers har försökt att obehörigt ta sig in i datorer har SÅRB tagit fram en rapport om "**Uppringda datorer**". Det är genom s k uppringda förbindelser som hackers har möjlighet att få kontakt med datorer. Rapporten har tagits fram av en arbetsgrupp i SIG/SEC för SÅRB:s räkning.

I rapporten ingår redogörelse för hur ett intrång går till, vilken skada ett intrång kan leda till, vilka skyddstekniker som finns och hur man kan utnyttja dessa för att skydda sig. I sina slutsatser pekar man på att det är brister i tekniken för identifikation av användare som utgör det stora hotet. Att hackers emellanåt faktiskt lyckas göra dataintrång beror genomgående på att den eller de personer som är ansvariga för registret och dess skydd på ett eller annat sätt missköter registerskyddet eller i vart fall inte tillvaratar tillgängliga skyddsmöjligheter. Rapporten innehåller åtskilliga råd om hur man skall sköta registret för att undvika intrång, som t ex att använda motringning, att spärra identiteter efter visst antal misslyckade påloggningsförsök, att inte tillåta användning av gamla lösenord, etc.

I rapporten ingår också en fyllig redogörelse för Televerkets olika tjänster, DATEL, DATAPAK, etc och en beskrivning av de i detta sammanhang aktuella säkerhetsegenskaperna hos de olika tjänsterna.

5.6.4 Slutsatser och rekommendationer

Risken för avlyssning av datakommunikationer är stor. Den som vill sända sekretessbelagda eller eljest känsliga data över Televerkets nät bör inte göra det utan att utnyttja kryptering.

Det finns stora möjligheter att störa trafiken över telenätet, genom genererad överbelastning som spärrar hela eller del av nätet, genom att obehörigt imitera en behörig terminal etc. Dessa risker måste beaktas av nätanvändarna. Risken för sabotage som fysiskt skadar näten är uppenbar.

Den som planerar och utvecklar system skall ha klart för sig vilken driftsäkerhet telenätet erbjuder och vilka möjligheter som det finns att köpa högre tillförlitlighet. En förutsättning för detta är att Televerket lämnar uppgift härom.

5.7 ADB i industrin

I handlingsplanen har SÅRB framhållit att man dittills i huvudsak endast berört frågor om sårbarhet i administrativa system medan industrins särskilda sårbarhetsproblem endast tagits upp marginellt.

Det är ett i många sammanhang omvittnat förhållande att industrin och då kanske särskilt den stora och viktiga verkstadsindustrin på senare år med CAD, CAM m fl tekniska tillämpningar gjort sig så beroende av en högrationell tillverkningsmetod att någon återvändo inte finns. Om elströmmen går eller datorn stannar enbart på grund av t ex en felprogrammering är i princip likgiltigt – produktion är i båda fallen omöjlig. Det finns flera skäl till detta – produktionen skulle bli orimligt arbetskrävande med manuella metoder. Dessa kan, om man ändå skulle vilja det, inte tillgripas av det skälet att nödvändig yrkeskunskap har försvunnit.

Vad SÅRB eller det organ som eventuellt kommer att uppta och fortsätta dess arbete kan göra åt denna situation synes i första hand vara att ge råd och information om sådana skyddsmetoder m m som allmänt är rekommendabla för att minska avbrottsriskerna.

Även om produktion med manuella metoder inte är möjlig finns det naturligtvis situationer där det kan vara ett starkt samhällsintresse att viss verksamhet kan fortsätta om än i begränsad omfattning inom en för totalförsvaret livsviktig funktion även om datorerna blir utslagna. SÅRB utesluter för sin del inte att sådana kris- och krigssituationer kan uppkomma och att tvångsåtgärder då måste tillgripas. En förutsättning härför är dock att man inom statsverket först klargör vilken produktion som är så betydelsefull för totalförsvaret att tvångsåtgärder kan bli aktuella. Sådan planering måste komma till stånd.

För övrigt instämmer SÅRB i den uppfattning som många näringslivsföreträdare har, nämligen att problemen med industrins sårbarhet bäst löses av näringslivet utan inblandning från staten.

Ett speciellt problem har ändå tagits upp i anslutning till frågan om näringlivets sårbarhet. Det är frågan om näringslivets uppgiftlämnande till statsorganen särskilt av sådana uppgifter som är av strategisk betydelse för uppgiftslämnaren och som man från näringslivshåll vill skall sekretessbeläggas. De särskilda problem som sammanhänger härmed har belysts i en PM som behandlas under rubriken 5.15 *Kassaskåpssäker sekretess och ADB.*

5.8 Undanförsel och förstöring av register

I SÅRB:s direktiv anges att SÅRB i samråd med den då arbetande datalagstiftningskommittén (DALK) skulle överväga frågan om rutiner och lagstiftning för förstöring av personregister. Enligt SÅRB:s uppfattning borde dock denna uppgift inte begränsas till att omfatta personregister utan även omfatta register som på annat sätt är av betydelse från totalförsvarssynpunkt. I enlighet härmed avlämnade SÅRB i augusti 1983 delbetänkandet "Undanförsel och förstöring av ADB-register" (Ds Fö 1983:8) till regeringen. I betänkandet konstaterar SÅRB att det inom området för beredskap redan i dag finns ett stort antal författningar och att området därför kan tyckas vara genomreglerat. Gemensamt för dessa bestämmelser är emellertid att de inte innehåller några närmare regler för hur vi i en kris- eller krigssituation skall förfara med från totalförsvarssynpunkt känsliga ADB-register.

SÅRB menar att de system/register som är av intresse för en angripare och

för vilka undanförsel- eller förstöringsrutiner därför bör utarbetas uppdelas i grupperna system/register som på grund av sitt innehåll är sårbart för

- rikets försvar och säkerhet
- rikets ekonomi och ekonomiska försvar
- personlig säkerhet

Vid ett ställningstagande till undanförsel eller förstöring måste i första hand beaktas om den registeransvarige skall bedriva verksamhet under krigsförhållanden. Beredningen menar att undanförsel och förstöring på intet sätt står i motsatsförhållande till planläggning för ADB-verksamhet i krig, utan att sådana åtgärder är en viktig beståndsdel av en beredskapsplanläggning i stort.

Delbetänkandet behandlar också frågor om hur undanförsel och förstöring praktiskt skall kunna utföras. Som alternativ till förstöring upptar SÅRB kryptering, som enligt beredningen uppvisar betydande fördelar från den synpunkten att registerinformationen finns kvar och att metoden kommer i fråga redan då ett register inrättas eller under pågående produktion och inte då det föreligger extrema samhällsförhållanden.

Vi får räkna med att en angripare har ett stort intresse av att komma över information i våra ADB-register. SÅRB menar att vi därför i betydligt större utsträckning än vad som sker i dag måste söka minska möjligheten till åtkomst av denna information. Detta kan enligt beredningen endast ske genom att statsmakterna och de som ansvarar för registren uppmärksammas på, att registren som de för kan vara känsliga för landets totalförsvar och att det krävs en planläggning om hur det skall förfaras med sådana register i en krigssituation. SÅRB förordade därför att det kommer till stånd en närmare reglering inom detta område så att undanförsel och förstöring av register blir en naturlig del av en beredskapsplanläggning i stort, vare sig fråga är om en planläggning för avveckling av verksamheten eller en planläggning för dess fortsatta bedrivande.

SÅRB föreslog i betänkandet lagreglering. Enligt förslaget skall registeransvarig (enligt den terminologi som tillämpas i datalagen) vara ansvarig för planläggning av undanförsel och förstöring. Planeringen skall ske i samråd med totalförsvarsmyndighet och anmälas till ÖEF och länsstyrelse. Författningsförslaget upptar vidare bestämmelser om hur och av vem beslut om undanförsel och förstöring skall fattas.

Delbetänkandet har remitterats. Bland remissinstanserna är den allmänna meningen att planläggningen för undanförsel och förstöring av ADB-register är eftersatt och att något måste göras åt detta. Majoriteten av remissinstanserna lämnar utan erinran eller tillstyrker beredningens förslag. Många har emellertid invändningar mot den författningstekniska lösningen och menar att det inte behövs någon ny lagstiftning utan att befintlig lagreglering eventuellt kompletterad med förtydliganden avseende ADB-register är tillfyllest.

Förslaget avsåg i första hand en modernisering av gällande regelverk men även en inventering av tekniska metoder för undanförsel och förstöring. Ytterligare överväganden ger emellertid vid handen att undanförsel kräver så omfattande planläggning, transportapparat och förberedda förvaringsutrymmen att undanförsel inte annat än i undantagsfall längre framstår som ett

realistiskt alternativ. Planläggning och rutiner för kryptering och förstöring saknas i sådan utsträckning att kraftfulla åtgärder är påkallade.SÅRB:s förslag bereds f n inom regeringskansliet.

5.9 ADB i krig

5.9.1 Direktiv

I SÅRB:s direktiv anfördes i anslutning till genomgången av SÅRB:s uppgifter att beredningen särskilt borde uppmärksamma "de säkerhetspolitiska konsekvenserna av olika åtgärder". I tilläggsdirektiven anfördes vidare att SÅRB senast den 2 maj 1985 till regeringen skulle "redovisa de erfarenheter från sitt arbete som kan utnyttjas som ett av de underlag som regeringen ställer till försvarskommitténs förfogande".

Försvarskommittén har enligt sina direktiv (Dir 1984:14) bl a till uppgift att lämna förslag till vilken säkerhet som skall eftersträvas inom ADB-området under kriser och krig, ställt i relation till den säkerhet som finns redan i fred.

5.9.2 ADB i kris och krig

I april 1985 beslutade SÅRB att lägga fram rapporten "ADB i kris och krig" för att uppfylla de krav som ställdes i direktiven. Det framhålls inledningsvis att rapporten som framtagits under loppet av ett par månader måste betraktas som en förstudie, att ytterligare arbete och analyser av dessa utomordentligt viktiga och svåra frågor kan komma att nyansera bedömningarna och ytterligare pröva behovet av åtgärder och möjligheterna att genomföra dem.

I rapporten konstateras att många för samhället viktiga funktioner är utomordentligt beroende av ett fungerande ADB-stöd. ADB-stödet är mycket sårbart och sårbarheten ökar om inte åtgärder vidtas. De allvarligaste svagheterna utgörs för närvarande av

- det stora utlandsberoendet av elektronikkomponenter
- den stora känsligheten för störningar i telekommunikationerna
- beroendet av nyckelpersonal samt
- de stora möjligheterna att skada ADB-systemen genom sabotage och vapenverkan.

ADB-säkerheten har inget egenvärde sägs det vidare. Den bör alltid utgå från de överordnade krav på funktion i kris och krig som ställs av den samhällssektor, eller motsvarande, där ADB-verksamheten ingår. I rapporten sägs också att olika samhällsfunktioner måste bli mera medvetna om sårbarhetsaspekterna, om sina uppgifter i krig och hur dessa skall planeras och förberedas.

Redan när utvecklingen av ett nytt ADB-system planeras, eller en större ändring i ett befintligt system, bör det klarläggas om det nya systemet eller befintliga system med vilket det integreras, skall användas i kris och krig. Genom en sårbarhetsanalys definieras sedan säkerhetskraven som grund för erforderliga skyddsåtgärder.

5.9.3 Slutsatser och rekommendationer

Rapporten "ADB i kris och krig" avslutas med förslag till ytterligare överväganden i en mera noggrann huvudstudie. Förslaget omfattar åtgärder som bör övervägas i en grundnivå respektive en tilläggsnivå och har följande lydelse:

Åtgärder för ADB-säkerhet som bör övervägas i en grundnivå:

- ADB-utvecklingen för särskilt samhällsviktiga system inriktas mot decentraliserade datakraftstrukturer samtidigt som sårbarhetsminskande åtgärder vidtas inom datakommunikationsområdet.
- Fortsatta ansträngningar görs för att standardisera såväl utrustning som programvara.
- Känslig datatrafik bör krypteras och framföras över förbindelser som är svåra att avlyssna och störa.
- Alla myndigheter, organ och industrier med uppgifter under kris och krig genomför en adekvat beredskapsplanering. Det bör finnas ett fackorgan med befogenhet att kontrollera denna planering.
- Säkerhetshöjande åtgärder, t ex förbättringar av det fysiska skyddet, vidtas i en omfattning som svarar mot funktionens betydelse i kris- och krigslägen.
- Uthålligheten förbättras genom lagerhållning av reservdelar, reservdrift och underhållskontrakt som även omfattar kris- och krigsskeden.
- Åtgärder vidtas för undanförsel eller förstöring av känsliga register i ett krisläge.
- Personalbehovet för planlagd ADB-drift i kris och krig klarläggs. Inom ramen för en övergripande syn på personalförsörjningen till totalförsvaret vidtas åtgärder för att tillförsäkra ADB-funktionerna erforderlig nyckelpersonal.
- Elektronikkomponenter som är väsentliga för totalförsvaret lagerhålls i en omfattning som svarar mot förbrukningen under bedömd längd av en allvarlig fredskris, följd av ett krigsskede.
- Funktioner som är avgörande för vår förmåga att uthärda en kris och att genomföra ett krig EMP-skyddas. Hit räknas:
  - Vissa civila och militära ledningsfunktioner.
  - Vissa system i militära förband.
  - Delar av el- och telenäten.

EMP-skyddet bör beaktas redan på planeringsstadiet. Det är som regel inte lönsamt att i efterhand ge anläggningar och system ett EMP-skydd.

Åtgärder som bör övervägas i en tilläggsnivå

- En kapacitet byggs upp och hålls i beredskap för begränsad produktion av sådana elektroniska standardkomponenter som är väsentliga för totalförsvaret.
- Ett säkerhetsnät överlagras det landsomfattande fiberoptiska nät som nu håller på att införas.

5.10 Utbildning

5.10.1 Utbildning för minskad sårbarhet

SÅRB har i handlingsplanen och även i andra sammanhang betonat att utbildning i ADB-säkerhet och sårbarhet är en förutsättning för ett ökat medvetande om riskerna och därmed för att på sikt kunna minska sårbarheten.

Det har tidigare rått en svår brist på utbildningsmaterial inom säkerhetsområdet lämpat för användning inom den allmänna skolan och andra utbildningsinstitutioner. Det har egentligen inte funnits något sådant material alls. SÅRB har därför sett det som en viktig uppgift att råda bot på denna brist genom att ta fram lämpligt utbildnings- och informationsmaterial.

5.10.2 ADB-säkerhet och sårbarhet – ett kompendium

Med hjälp av en arbetsgrupp sammansatt av kunniga och välinformerade personer som arbetar inom olika utbildningsformer – privata och statliga, högre och lägre har SÅRB under 1984/85 tagit fram ett kompendium avsett för användning inom olika skolformer och möjligt att anpassa för såväl mindre som mera kvalificerad undervisning.

Kompendiet har testats i skolmiljö och befunnits fylla ett stort behov och i sak vara väl lämpat för sitt ändamål.

Emellertid måste kompendiet också på lämpligt sätt marknadsföras eller föras ut för att få en bred användning. I detta syfte har ett samarbete inletts med Riksdataförbundet och Utbildningsproduktion AB. Avsikten är att pedagogiskt förbättra kompendiet, att förse det med handledaranvisningar och andra studiehjälpmedel och därefter lansera det. Det kompletterade kompendiet kommer att ges ut i början av 1986.

5.10.3 Den sårbara datorn

I den omfattande planeringen av utbyggnaden av ADB-undervisningen i skolan har den personliga integriteten, sårbarhet och säkerhet fått en mycket undanskymd placering. För att i någon mån råda bot på detta har SÅRB tagit fram en broschyr och en affisch med i stort sett samma innehåll, som informerar om ämnet och är anpassad för att kunna delas ut till och läsas av elever. Utbildningsdepartementet och skolöverstyrelsen har trätt in och svarat för kostnaden för att ta fram och till skolorna distribuera 10 000 ex av broschyren och ett par tusen affischer. Efterfrågan på ett sådant lättsmält och kortfattat informationsmaterial har f ö varit stor även från andra håll än skolan.

5.11 Kryptering

5.11.1 Bakgrund

National Bureau of Standards i USA antog 1977 en av IBM utvecklad kryptoalgoritm som Federal Information Processing Standard, FIPS. Algoritmen, som kallas Data Encryption Standard, DES är påbjuden att användas för alla federala data som behöver skyddas. Att ha en helt öppen och offentlig kryptoalgoritm och t o m göra den till standard var då en anmärkningsvärd nyhet. Tanken var förstås att ha en öppen algoritm men i gengäld en strängt hemlighållen nyckel.

DES-algoritmen väckte stort intresse även icke-federalt och utanför USA. ANSI, som är USA:s nationella standardiseringsorgan godtog DES-algoritmen som standard 1981 men döpte om den till DEA, Data Encryption Algorithm.

Under 1983 blev det aktuellt att göra DEA till europeisk standard i ISO. Därmed måste även Sverige och Standardiseringskommissionen, SIS ta ställning till om DEA skulle antas som svensk standard. Även av andra skäl blev kryptering ett högaktuellt ämne. Bl a visade Televerkets riskanalyser att datakommunikationen närmast är vidöppen för obehörig avlyssning och avtappning av data. Någon annan metod att skydda hemliga data i datakommunikationsnätet än kryptering finns inte.

Mot denna bakgrund beslöt SIS och sedermera av motsvarande skäl SÅRB att något måste göras. Det mest naturliga var att på lämpligt sätt sprida kunskap om krypteringsteori, -tekniker och -möjligheter till en bredare krets av människor än det fåtal kryptoexperter som hittills haft monopol på sakkunskap inom området.

5.11.2 Hjälpredan

Under 1984 beslöt SÅRB och SIS och sedermera även Riksdataförbundet, med vilket samarbete söktes, att satsa på att utveckla en handbok eller vad som kom att kallas en hjälpreda i kryptering. Boken skulle rikta sig till och utgöra vägledning för projektledare och systemerare och kanske också beslutsfattare som har att besluta om systemutformning och där ställningstagande i dataskyddsfrågor kan bli avgörande för vilken systemlösning som väljs. Projektet finansierades genom bidrag från myndigheter och företag. Boken trycktes av SIS som teknisk rapport. RDF har hjälpt till med marknadsföringen. Boken heter "Kryptering i ADB-system. Praktisk hjälpreda för beslutsfattare och systemerare".

5.11.3 Slutsatser och rekommendationer

Det är uppenbart att kraven på skydd av data som sänds – antingen det sker på telenätet eller med flyg/tåg/bil på magnetband – snabbt håller på att skärpas. Inom några få år kommer det att framstå som icke godtagbart att sända sekretessbelagda eller eljest känsliga data i okrypterad form. Vi kan med säkerhet emotse en utveckling som innebär en snabb spridning av

krypteringsmetoder, – standarder, – tillämpningar. Något annat alternativ till kryptering än att avstå från datakommunikation finns inte.

5.12 Röjande signaler

Även om militära experter känt till förekomsten av s k röjande signaler, RÖS under lång tid är det först under de senaste 3-4 åren som RÖS kommit att betraktas som riskfaktor även i civila sammanhang.

Källorna för RÖS kan vara ljud som avges av maskiner och kan uppfångas av obehöriga, elektromagnetiska signaler, videosignaler, radiovågor och överlagrade signaler som leds ut bl a i kraftnät. Kraven på RÖS-skydd varierar naturligtvis beroende på sekretessgraden hos behandlade data. Skydd mot RÖS kan åstadkommas genom byggnadstekniska åtgärder, skärmning, avstörningsfilter, ljudisolering.

Om dessa frågor handlar informationsskriften "Läckande datorer – en information om RÖS" som SÅRB och Brottsförebyggande rådet gemensamt bekostade och producerade år 1984. Skriften har rönt mycket stor efterfrågan och hittills distribuerats i närmare 15 000 exemplar.

5.13 Kravspecifikation behörighetskontrollsystem BKS

5.13.1 Ofullständiga BKS

De första behörighetskontrollsystemen för datorer togs fram i mitten på 70-talet. De hade börjat efterfrågas bl a som en följd av att datainspektionen började ställa högre krav på skyddet av känsliga personregister. Numera finns en rik flora av BKS – de flesta levererade av datorleverantörsföretag.

Användare har traditionellt en svag ställning i förhållandet till de stora, multinationella företag som alltid och alltjämt dominerar datormarknaden. Användarna har godtagit de BKS som företagen levererat och utsikterna att få gehör för lite mera udda önskemål har varit obefintliga. Enligt vissa användares mening har tillgängliga BKS inte varit bra, de är dessutom svåra att jämföra med varandra eftersom det saknats ett gemensamt språk eller en gemensam norm för beskrivning och kravspecifikationer på BKS. Många kvalificerade användare bl a representerade av SIG-SEC, en särskild intressegrupp för ADB-säkerhetsfrågor inom Svenska samfundet för Informationsbehandling, SSI, har tröttnat på det underläge man haft och har gentemot datorleverantörerna. Man vill gemensamt enas om och ställa sig bakom en beskrivningsmodell, norm, eller kravspecifikation för BKS, som BKS-leverantörerna framdeles skall tvingas relatera sina produkter till. Härigenom låter man sig inte längre nöja med *att* en leverantör tillhandahåller ett BKS utan kan också bestämma *hur* ett sådant system skall fungera för att kunna godtas.

5.13.2 Säkerhetskrav på datorer och operativsystem

1984 beslutade SÅRB att uppdra åt SIG-SEC att i samarbete med beredningen ta fram "Säkerhetskrav på datorer och operativsystem". Projektet omfattar i huvudsak krav på BKS men innefattar även sådana krav på säkerhetsarkitektur m m som är av betydelse för ett väl fungerande BKS. Rapporten behandlar följande avsnitt,

- Säkerhetsarkitektur
- Identifiering
- Behörighetskontroll
- Rapportering
- Back-up och recovery

5.13.3 Slutsatser och rekommendationer

Det är viktigt och har ju också ingått i SÅRB:s åligganden att bidra till att öka användarkompetensen i fråga om ADB-säkerhet. Det är också viktigt och av betydelse för kompetensutvecklingen att dataanvändarna går samman och enas i sina krav på företag som levererar hårdvara, mjukvara och datatjänster. SIG-SEC med sina f n drygt hundratalet ADB-säkerhetsansvariga från myndigheter och företag i samarbete med och uppbackade av SÅRB utgör en kvalificerad och slagkraftig kravställare som även stora datorleverantörer måste ta på allvar.

Det finns, som slutsatsvis berörs även i andra avsnitt i slutrapporten, grund för uppfattningen att befintliga ADB-säkerhetsmetoder i flera avseenden är otillräckliga för att skydda känslig information. Följden härav *kan* bli allvarliga begränsningar i den fortsatta datoriseringen. Skall vi undgå att hamna i en sådan situation är det viktigt att vi förbättrar de gamla och utvecklar nya ADB-säkerhetsmetoder.

5.14 Offentlighetsprincipen, ADB och sårbarhet

5.14.1 Bakgrund

Under någon vecka sommaren 1984 fördes i massmedia en livlig debatt om offentlighetsprincipens betydelse för bl a den militära säkerheten. Man menade att offentlighetsprincipen medger sådan tillgång till uppgifter i dataregister av betydelse för försvaret, att den militära säkerheten kan äventyras. Som ett exempel nämndes att man genom fastighetsdatasystemet kan få uppgift om vilka fastigheter som ägs av militära intressenter och som alltså kan antas ha särskild betydelse för försvaret. Som ett annat exempel nämndes att man genom den s k vägdatabanken kan få uppgifter om olika broars uppbyggnad, hållfasthet m m och om de är förberedda för att sprängas i krig. Problemet är enligt debatten att offentlighetsprincipen ger för *vid* rätt till insyn i dataregistren och att gällande sekretessregler inte ger tillräckligt skydd mot de säkerhets- och sårbarhetsrisker detta innebär.

Mot bakgrund härav beslutade SÅRB att undersöka om debatten gett en

korrekt bild av offentlighetsprincipens effekter. I december 1984 presenterades en PM härom.

5.14.2 Promemorian

I PM redogörs för gällande rätt. Några myndigheter, bl a de inledningsvis berörda, Centralnämnden för fastighetsdata, CFD och vägverket ger sin egen syn på problemen. Det framgår att massmedias uppgifter allmänt sett är överdrivet hårdragna, att sådant uppgiftslämnande som nämns i exemplen i några fall aldrig varit aktuella och om de hade blivit det, med säkerhet föranlett noggrann prövning.

Sammanfattningsvis sägs i PM-konsultrapporten följande

Mot bakgrund av våra erfarenheter från intervjuerna tror vi inte att vaksamheten och tillämpningen av försvarssekretessregeln utgör något problem inom försvarsmakten. Visserligen finns nog en viss tveksamhet om vad offentlighetsprincipen innebär i ADB-miljö men detta hindrar inte att man är ytterst vaksam när det gäller tillämpningen av sekretessreglerna.

När det gäller den civila statsförvaltningen tror vi däremot att det finns ett stort informationsbehov både vad avser offentlighetsprincipens tillämpning i ADB-miljö allmänt sett och i vad mån försvarssekretessen kan bli tillämplig på den enskilda myndighetens verksamhet.

– – – – –

Vi vill ifrågasätta om inte detaljerade sammanställningar av statsförvaltningens ADB-användning, såsom statskontorets rapport (1982:11) Statliga ADB-system och FRI:s systemkatalog, är olämpliga från sårbarhetssynpunkt.

Det föreslogs också att SÅRB skulle verka för att någon form av informationsbroschyr i ämnet skulle tas fram för den civila statsförvaltningen.

5.14.3 SÅRB:s beslut

SÅRB beslutade att genast delge regeringen promemorian. Till denna fogades ett missiv i vilket SÅRB redogör för sin ståndpunkt enligt det följande:

SÅRB delar uppfattningen i promemorian att läget, sett från militära säkerhetsaspekter, inte kan betecknas som alarmerande. Med hänsyn härtill är enligt SÅRB:s uppfattning några omedelbara och mer ingripande åtgärder för närvarande inte påkallade.

SÅRB anser dock att vissa åtgärder kan vara motiverade för att höja medvetenheten om försvarssekretessen inom den civila statsförvaltningen i syfte att inte i onödan underlätta för den som söker få del av uppgifter i datasystemen, som var för sig eller i sammanställd form kan vara känsliga från försvarssynpunkt. SÅRB föreslår därför, i likhet med det anförda i promemorian att promemorian för beaktande överlämnas till Data- och offentlighetskommittén, DOK, Ju 1984:06.

SÅRB anser också att förslaget om en informationsbroschyr i ämnet offentlighetsprincipen, ADB och försvarssekretessen bör prövas, liksom nyttan vägd mot försvarssekretessaspekter av de kataloger över ADB-system som statskontoret och försvarets rationaliseringsinstitut ger ut.

SÅRB pekade i skrivelsen på att det finns ett antal andra frågor kring offentlighet, sekretess och ADB än den som behandlades i promemorian och som också förtjänar att uppmärksammas från sårbarhetssynpunkt.

En sådan fråga gäller risken för att industrispionage och andra liknande, otillbörliga aktiviteter underlättas genom myndigheternas omfattande insamling av uppgifter från företagen och den insyn i företagens verksamhet detta kan ge anledning till. En annan fråga gäller risken för att känsliga och kanske sekretessbelagda företagsuppgifter i alltför hög grad sprids inom myndigheterna bl a genom de allt fler terminaler, som blir vanliga i myndigheternas ADB-system och som ökar tillgänglighet och behörighet till informationen.

Dessa frågor behandlas i avsnitt 5.15.

5.14.4 Regeringens beslut

I ett regeringsbeslut i oktober 1985 meddelas *att* statskontoret uttalat att någon ny utgåva av den aktuella rapporten (1982:11) Statliga ADB-system inte planeras, *att* ÖB anfört att någon ny utgåva av försvarets rationaliseringsinstituts systemkatalog inte bör ges ut och *att* SÅRB:s promemoria överlämnats till justitieministern.

I ett regeringsbeslut den 28 november 1985 sägs att rikspolisstyrelsen och överbefälhavaren efter remiss yttrat sig över SÅRB:s promemoria. Regeringen beslutade följande,

Med hänvisning till 7 § förordningen (1981:421) om säkerhetsskyddet vid statliga myndigheter beslutar regeringen att överlämna SÅRB:s skrivelse till rikspolisstyrelsen såvitt gäller utarbetande av en informationsbroschyr angående offentlighetsprinipen, ADB och försvarssekretessen.

– – – – –

Regeringen beslutar att överlämna SÅRB:s framställning i övriga delar jämte promemorian till data- och offentlighetskommittén.

Samma dag beslutade regeringen om en förordning om ändring i förordningen (1981:421) om säkerhetsskyddet vid statliga myndigheter. I förordningen införs en ny paragraf, 4a §, av följande lydelse

4 a § Innan en myndighet inrättar ett register, som skall föras med hjälp av automatisk databehandling och som kan förutses komma att innehålla uppgifter av betydelse för totalförsvaret eller rikets säkerhet i övrigt, skall myndigheten samråda med överbefälhavaren eller, om uppgifternas natur ger anledning till det, rikspolisstyrelsen.

Denna förordning träder i kraft den 1 januari 1986.

I detta sammanhang ter det sig naturligt för SÅRB att peka på myndigheternas mycket omfattande uppgiftsinsamling. SÅRB anser att de möjligheter som modern ADB-teknik ger ej sällan används på ett sätt som kan äventyra säkerheten. Avvägning mellan nyttan av insamlade uppgifter och riskerna därmed sker icke alltid.

Aktuell lagstiftning innefattar normalt inga restriktioner i myndigheternas rätt att inhämta uppgifter. I exempelvis lagen om hälso- och miljöfarliga

varor sägs i 12§: "Tillsynsmyndighet har rätt att efter anfordran erhålla upplysningar och handlingar som behövs för tillsynen enligt denna lag". Besvärsmöjlighet finns normalt ej.

En ökad restriktivitet vid uppgiftinsamlingen är således enligt SÅRB:s mening befogad.

Myndigheternas handel med uppgifter växer snabbt och är enligt SÅRB:s mening en källa till oro. Man kan inte bortse från att det råder ett samband mellan omfattningen av uppgiftinsamlingen å ena sidan och myndigheternas försäljningsverksamhet å den andra.

Mot denna bakgrund finner SÅRB det vara angeläget att regeringen snarast låter utarbeta riktlinjer för försäljningsverksamheten, som är ägnade att minska företagens uttag av uppgifter för kommersiella ändamål. Det är enligt SÅRB:s mening otillfredsställande att denna verksamhet – med något enstaka undantag – tillåts fortgå utan stöd i lag.

5.14.5 Slutsatser och rekommendationer

Genom åtgärder som här ovan redovisats har möjligheterna att kontrollera datoriseringens effekter för totalförsvaret förbättrats något. Det återstår emellertid att skaffa överblick över datoriseringen i samhället i övrigt, så att inte viktiga säkerhetsintressen äventyras.

Riktlinjer för försäljningsverksamheten av uppgifter bör snarast utarbetas. I den utsträckning försäljning kommer att tillåtas bör denna handel uttryckligen regleras i lag.

5.15 Kassaskåpssäker ADB?

5.15.1 Bakgrund

I samband med bl a arbetet med projektet Offentlighetsprincipen, ADB och sårbarhet och även under arbetet med ADB i industrin har frågan väckts, särskilt från näringslivsföreträdare, om vilka effekter det snabbt ökande antalet terminalbaserade ADB-system hos myndigheterna i praktiken får på det faktiska sekretesskyddet.

5.15.2 Tryckfrihet och sekretess

Enligt tryckfrihetsförordningen har i princip var och en rätt att ta del av allmänna handlingar. Med allmän handling menas både framställning i skrift eller bild och s k "upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel". Med det sistnämnda avses bl a register som förs med ADB t ex på magnetband. Handling är allmän om den förvaras hos myndighet och anses som inkommen till eller upprättad hos myndighet.

Undantagen från denna grundlagsfästa rätt att ta del av allmänna handlingar hos en myndighet finns i sekretesslagen. En begäran om utlämnande av uppgift för vilken sekretess gäller skall från fall till fall prövas mot bakgrund av det "skaderekvisit" som gäller i förekommande fall.

Den lagtekniska konstruktion för vilken här kortfattat redogjorts tillkom långt före datorerna – i sina grunddrag för mer än 200 år sedan. Då fanns inga datorer. Utan att gå så långt tillbaka i tiden kan man dock, genom att studera nu gällande föreskrifter, anvisningar och råd som gäller tillämpningen av sekretesslagen, sekretessförordningen, etc få en uppfattning om vilken vikt lagstiftarna lagt vid att sekretesskyddade uppgifter faktiskt hindras från att spridas till obehöriga.

5.15.3 Föreskrifter, råd och anvisningar

Av Föreskrifter, anvisningar och allmänna råd om tillämpningen av säkerhetsskyddsförordningen (FA SÄK 1982) framgår de rigorösa regler som gäller för hemliga handlingars hemligbeteckning, registrering, kvittering vid utlämnande, kopiering, förvaring, inventering, gallring och arkivering. Som bilaga ingår i FA SÄK f ö också "Anvisningar för säkerhetsskydd vid automatisk databehandling". Dessa anvisningar är dock mera allmänt hållna och av helt annan karaktär än de som gäller traditionella handlingar.

5.15.4 Sårbarhetsproblem

De frågor som SÅRB mot denna bakgrund ville belysa var följande. För det första kan ifrågasättas om det sekretesskydd som sekretesslagen i förekommande fall förutsätter överhuvudtaget tekniskt sett kan uppnås när informationen lagras på ADB-medium och blir tillgänglig i datoriserade informationsnät. Särskilt gäller detta system av den typ som är vanlig i statsverket med central dator och ett antal direkt via telenätet anslutna terminaler.

Det är f ö inte alltid som de tekniska skyddsmetoder som ändå finns tillgängliga verkligen utnyttjas. I många system som omfattar uppgifter för vilka sekretess råder blir behörighetskontrollen illusorisk eftersom den ej är individuell. Till person knuten behörighetskontroll är en förutsättning för att ett rimligt mått av restriktivitet i uppgiftlämnandet skall anses gälla. För det andra har det ifrågasatts om inte den frikostiga tilldelningen av terminaler och det ibland mycket stora antalet behöriga användare kan innebära att sekretesskyddet urholkas eller kanske rentav måste betraktas som satt ur spel. Ett exempel kan vara de polisregister, för vilka rikspolisstyrelsen är registeransvarig. Å ena sidan anses dessa register så känsliga att särskild lagreglering ansetts nödvändig för att förhindra obehörig användning (lag (1965:94) om polisregister m m). Å andra sidan är i vart fall vissa av dessa åtkomliga helt eller delvis för ca 20 000 anställda i polisväsendet via flera hundra terminaler. Under 1985 har enligt uppgift fem tjänstemän dömts för att ha missbrukat sin behörighet. I realiteten måste man utgå från att antalet syndare är många, många flera. En uppgift som 20 000 människor nästintill utan tekniska restriktioner kan ta del av – kan den anses vara hemlig?

5.15.5 Kassaskåpssäker ADB-sekretess?

För att belysa de här nämnda frågorna, särskilt såvitt gäller känsliga uppgifter om företag engagerades experterna Torbjörn Nilsson, statskontoret och Lars

Lindgren, SHB, som även svarade för utredningen om offentlighetsprincipen etc (avsnitt 5.14). De ansåg inte att deras begränsade undersökning gav vid handen att sekretesskyddet för företagsuppgifter är avsevärt sämre i datormiljö än i äldre miljöer men pekade på att skadan vid obehörig åtkomst kan antas bli betydligt större när det gäller ADB-register, eftersom man då kan komma att få tillgång till betydande informationsmängder. De gjorde härutöver följande intressanta iakttagelser.

Författarna har särskilt studerat produktkontrollnämnden och det uppgiftslämnande som nämnden begär för sitt produktregister. Man har också intervjuat företag som är uppgiftlämnare till registret och bl a noterat följande,

- att de intervjuade företagen inte litar på att de uppgifter man lämnar till staten endast används för ursprungligen avsett ändamål,
- att man inte litar på att de statstjänstemän som ansvarar för inlämnade uppgifter är tillräckligt sakkunniga för att kunna göra en korrekt skadebedömning vid ett ifrågasatt utlämnande,
- att företagen av ovan nämnda skäl underlåter att lämna uppgifter som man bedömer vara särskilt känsliga vilket försämrar datakvaliteten i de aktuella registren,
- att företagen saknar förståelse för de syften, som angivits för att begära in uppgifter.

5.15.6 Integration och spridningseffekter

Integreringen mellan olika informationssystem leder till att information stundom sprids långt från den källa, där medvetenheten om skyddsvärdet är tillfredsställande, till organisationer som mer eller mindre saknar kunskap om skyddsbehovet. Med moderna programmeringsspråk och informationssökningssystem kan helt oförutsebara konstellationer av data tas fram och spridas. Detta ökar i betydande grad svårigheten att skydda känsliga uppgifter.

5.15.7 Slutsatser och rekommendationer

De säkerhets- och kontrollmetoder för ADB som idag finns tillgängliga ger inte godtagbart skydd av hemliga eller eljest känsliga data särskilt inte i tillämpningar med datakommunikation via publika nät. Metodutveckling krävs för att förbättra skyddet.

Det finns anledning överväga större restriktivitet i uppgiftspridningen. Det finns system som endast lämpar sig för in-house-bearbetning och där uppgiftspridning till terminaler via allmänna nät med hänsyn till riskerna inte bör godtas.

Större restriktivitet i fråga om spridning av behörighet att ta del av ADB-registrerade hemliga uppgifter bör övervägas.

5.16 Inventering av ADB-säkerhet

SÅRB har i enlighet med sina direktiv haft att "inventera hittillsvarande arbete inom området ADB-säkerhet, analysera användbarheten av detta material samt att i samverkan med främst statskontoret föreslå förbättringar och kompletteringar i de fall beredningen anser det vara motiverat".

5.16.1 Konsultrapporten

Under 1984/85 har i enlighet härmed en kartläggning gjorts av sparbankernas revisionsbyrå SPAREV AB på uppdrag av statskontoret och i samråd med SÅRB. Kartläggningsarbetet utfördes av konsulten Tage Magnusson, som under större delen av 70-talet för statskontoret arbetat med ADB-säkerhetsfrågor.

Kartläggningen gjordes i form av intervjuer med ett stort antal användaremyndigheter och – företag, med företag som levererar datorer och annan "hårdvara", tjänsteföretag och organisationer inom konsultbranschen, som arbetar med utveckling, utbildning, försäkring etc

Konsulten har vidare inventerat och studerat befintlig och tillgänglig huvudsakligen svensk litteratur inom området.

Kartläggningen resulterade i dels ett omfattande material insamlat i samband med intervjuerna, dels en ca 50-sidig promemoria i vilken resultatet av intervjuer och litteraturstudier sammanfattas och dokumenteras.

Konsultrapporten avslutas med sammanfattande analys och slutsatser av kartläggningen. Sammanfattningsvis sägs följande.

- Metodanvisningar till vägledning för den som skall bygga upp sitt ADB-skydd är viktiga och saknas ofta.
- Avstämnings- och datakvalitetskontroller är ofta otillräckliga. Tillgängliga kontrolltekniker bör sammanställas och presenteras.
- Ofta är maskinella och personella databehandlingsresurser för snålt tilltagna. Det saknas reserver. Allmänt sett är funktionsskyddsmetoder dåligt beskrivna. Åtskilligt mera finns att göra.
- Behörighetssystemen ger för dåligt skydd och är emellanåt av den arten att de snarare försämrar än förbättrar säkerheten genom att de kringgås av personalen. En mera kvalificerad kravspecifikation är önskvärd.
- Reservrutiner och andra reservförfaranden som säkerhetskopiering och säkerhetsarkivering försummas ofta. Här finns behov av en praktisk hjälpreda.
- Säkerhetsorganisatoriska problem, ansvarsfrågor, planeringsfrågor och ADB-säkerhetschefens roll måste få en bättre belysning.
- Policy och riktlinjer för säkerhetsarbetet är ofta otillräckliga.
- Kryptering är en viktig dataskyddsmetod men det saknas sådan dokumentation att en vanlig användare själv kan bedöma behov och möjligheter.
- Begreppsnomenklaturen inom ADB-säkerhetsområdet är föråldrad och bör ses över.

5.16.2 ADB-säkerhetens begreppsapparat

Av hävd har ADB-säkerheten särskilt kommit att betraktas som en samling skyddsmetoder eller -åtgärder. Ett exempel på detta är den terminologistandard avseende ADB-säkerhet som SIS fastställde 1981. I ett inledande avsnitt redogörs för den systematik eller ram i vilken de enskilda termerna sorteras in. Det nämns i standarden att i varje steg i databehandlingen kan risken för skada och skadans omfattning minskas genom skyddsåtgärder, som kan fördelas efter olika principer

- Indelning efter var åtgärden vidtas,
  - i maskinvaran
  - i programvaran
  - i organisationen
  - i systemets omgivning
- Indelning efter den effekt som åtgärden är avsedd att ge. Effekten kan vara
  - förebyggande
  - begränsande
  - återställande
  - rapporterande
- Indelning efter det objekt som åtgärden är avsedd att skydda. Motsvarande skydd kan vara
  - kapitalskydd
  - funktionskydd
  - dataskydd
  - datakvalitetsskydd

En viss skyddsåtgärd kan samtidigt ge effekter av flera slag eller vara avsedd att skydda flera objekt.

Man har naturligtvis alltid varit på det klara med att skydds- och säkerhetsåtgärder inte kan eller bör sättas in utan att man först har granskat och värderat riskerna. Men metodproblemen vid riskanalys har tidigare rönt mycket litet uppmärksamhet. Intuitionen har i stor utsträckning fått vara vägledande vid val av säkerhetsåtgärder.

Genom tillkomsten av SBA-metoden ändrades detta. SBA-metoden som utvecklades åren 1982/83 är en förhållandevis enkel riskanalysmetod som rätt använd ger underlag för en rationell bedömning av var skyddsåtgärder bör sättas in.

Risk- eller sårbarhetsanalys är alltså den ena och skydds- eller säkerhetsmetoder och -åtgärder den andra delen av ADB-säkerheten. Utan sårbarhetsanalys är säkerhetsåtgärder svåra att prioritera – utan efterföljande överväganden om säkerhetsåtgärder är sårbarhetsanalysen meningslös.

Oavsett vilka säkerhetsåtgärder som vidtas kan riskerna för svåra skador aldrig helt elimineras. En förödande brand i datacentralen kan förebyggas genom byggnadstekniska åtgärder, genom att använda icke brännbara material o s v. Branden kan begränsas genom släckningsanordningar etc. Det finns alltså en mängd åtgärder som kan vidtas. Ändå sker förödande bränder. Genom katastrofplanering – back-up-avtal, särskilda leveransavtal med datorleverantör o s v försöker man även att gardera sig mot att

utslagning av datakraften får katastrofala följder.

En kategori av åtgärder som på grund av sin omfattning och sin särskilda tillämpningsinriktade karaktär knappast kan inrangeras bland det som vi här har kallat skydds- och säkerhetsåtgärder är att förbereda sig så att man kan hålla – inte databehandlingen – utan de ADB-stödda verksamheterna, produktionen, försäljningen, in- och utbetalningarna o s v igång i datorlöst tillstånd. Kanske med avsevärt reducerad service men ändå på sparlåga till dess databehandlingen åter kommer igång. Ett exempel: Hur skall SJ kunna boka platser om och under den tid som bokningssystemet är utslaget? Denna typ av frågor utgör en tredje komponent i säkerheten. Den första är således risk- och sårbarhetsanalysen, den andra är skydds- och säkerhetsåtgärderna och den tredje är planeringen av verksamheten i datorlöst tillstånd.

SÅRB har i annat sammanhang fört fram synpunkten att ADB-säkerhet inte enbart är en fråga om kostnadskrävande skyddsåtgärder avsedda att minska diffusa risker. ADB-säkerhet är också en effektivitetsfråga. En mycket stor del av riskerna för oavsiktliga fel och misstag kan exempelvis elimineras genom bättre ordning på arbetsplatsen, bättre arbetsledning och arbetsdisciplin, bättre rekrytering och utbildning och inte minst lämplig systemutformning. Det är fullt möjligt och rimligt – och i själva verket en förutsättning för att mera traditionella säkerhetsåtgärder skall vara meningsfulla – att betrakta systemteknik och organisation i ett säkerhetsperspektiv. Försummar man att beakta dessa förhållanden är det inte stor mening med att sätta in de mera traditionella säkerhetsåtgärderna.

Att ADB-säkerhet och effektivitet hör ihop bekräftas f ö också av flera stora ADB-driftorganisationer, t ex Televerket och Dafa.

Konsulten har i sin rapport huvudsakligen uppehållit sig vid frågor om förekomsten och i vissa fall avsaknaden av säkerhets- och skyddsåtgärder. I rapporten diskuteras också definitionsfrågorna. Det framhålls att det är otillfredsställande med en alltför begränsad definition som inte ger någon vägledning för att bedöma om de skydd man sätter in är tillräckliga och lämpliga. Det framhålls också att t ex Föreningen Auktoriserade Revisorer, FAR tillämpar en definition av begreppet internkontroll som ligger nära det SÅRB menar bör omfattas av begreppet ADB-säkerhet. FAR anser således att internkontrollen – säkerheten *dels* omfattar sådana kontroller som säkerställer en riktig och fullständig redovisning men *dels* också omfattar effektiviteten i verksamheten. Med det sistnämnda avses förvaltningsrevisionella kontroller som främst befrämjar effektiviteten och säkerställer att ett företags resurser disponeras endast i enlighet med styrelsens och verkställande direktörens intentioner.

Konsulten har mot denna bakgrund ansett det vara motiverat att se över och eventuellt modifiera nuvarande standardiserade begreppsmodell.

5.16.3 Slutsatser och rekommendationer

Metodutveckling är en viktig del av utvecklingen inom säkerhetsområdet. Av de åtgärdsområden som nämns i konsultrapporten har några behandlats av SÅRB. Det gäller bl a krav på behörighetskontrollsystem, säkerhetsorganisatoriska problem och kryptering. Övriga nämnda åtgärdsområden bör som föreslås tas upp för metodutveckling. Begreppsapparaten är enligt

SÅRB:s mening mogen för översyn och revision. Särskilt bör sårbarhetsanalysen, den tillämpningsinriktade avbrottsplaneringen, betydelsen av ordning och reda och lämplig organisation liksom sambandet mellan ADB-säkerhet och effektivitet infogas i teoribildningen.

6 Resultat och förslag

6.1 Resultat och erfarenheter

Som tidigare nämnts konstaterade sårbarhetskommittén i sitt slutbetänkande att sårbarheten hade blivit oacceptabelt hög och att den skulle öka ytterligare om inte motåtgärder vidtogs. SÅRK föreslog lagreglering, vilket emellertid avvisades. I stället tillsattes SÅRB för att på frivillig väg försöka minska samhällets sårbarhet. SÅRB skulle genom rådgivning och information öka medvetenheten hos beslutsfattare och datoranvändare. Genom olika projekt skulle man ta fram metoder och hjälpmedel för att öka säkerheten.

SÅRB har under årens lopp lämnat flera bidrag till metodutvecklingen inom ADB-säkerhetsområdet. De rapporter som SÅRB efter hand har tagit fram och offentliggjort har genomgående fått ett bra mottagande, som generellt sett tyder på en stark efterfrågan och stort behov av nya och bättre metoder och hjälpmedel inom området.

6.1.1 Samarbete – ett värde i sig

De olika i SÅRB:s projekt medverkande myndigheterna, företagen och organisationerna har ställt upp i projektarbetet inte bara med pengar utan också med personella resurser. På så vis har man vunnit den stora fördelen att projektresultaten fått en omedelbar praktisk spridning och förankring ute hos myndigheter och i näringslivet. I SBA-projektet medverkade t ex inte mindre än ett 40-tal personer i olika arbets- och referensgrupper. Det samarbete som således kommit till stånd mellan staten, kommuner och näringslivet och med SÅRB som katalysator har inte bara stora ekonomiska fördelar. Ett sådant samarbete har ett stort värde i sig. Dubbelarbete undviks och de olika sektorerna kan dra ömsesidig nytta av de inblickar man kan få i andra samhällssektorer. En bättre förståelse och ett ökat förtroende mellan företrädare för myndigheter och näringsliv är någonting som alla har nytta och glädje av. Samarbete gör det också möjligt att utveckla ett gemensamt synsätt – med en framväxande etisk norm som följd. I några av SÅRB:s projekt har ett liknande samarbete och utbyte med universitets- och forskarvärlden förekommit, särskilt med Linköpings universitet. Allmänt sett hade ett vidare samarbete dock varit önskvärt.

6.1.2 Ökande medvetande

En summering av uppnådda resultat och erfarenheter ger anledning konstatera att många ADB-säkerhets- och sårbarhetsfrågor kan hanteras på frivillig väg utan att lagstiftning skall behöva tillgripas. Medvetandet om sårbarhetsproblemen och nödvändigheten att göra något åt dem är idag bättre än för några år sedan. En bidragande orsak härtill har varit den omfattande publiciteten kring säkerhetsfrågorna under senare år. Om det ökade medvetandet och intresset vittnar det förhållandet att företag och organisationer i så hög grad har bidragit till finansieringen av SÅRB:s projekt. Ett annat tecken är alla de företag som under senare år bildats och växt upp inom ADB-säkerhetsbranschen.

Totalt sett har medvetandet om problemen ökat vilket naturligtvis är positivt. Däremot är det tveksamt om den ökade medvetenheten hittills fått tillräckligt genomslag. Situationen förbättras dock fortlöpande.

Ser man tillbaka ett tiotal år kan man konstatera en klar attitydförändring. Ännu för 10 år sedan planerades datacentraler med skyltfönster ut mot gatan. För 10 år sedan var "closed-shop"-drift ingen självklarhet ens i stora datacentraler och behörighetskontrollsystem var i stort sett okända. I dag är inställningen en annan och säkerhetsmedvetandet bättre. Ett fortsatt arbete i syfte att reducera sårbarheten och öka säkerheten kan säkert åstadkomma en motsvarande utveckling, under den kommande 10-årsperioden. Men samtidigt fortsätter datoriseringen och vårt beroende av datorer ökar. Vad den sammanlagda effekten blir 1995 är knappast möjligt att förutse. Vad vi säkert vet är dock att datoriseringen sprider sig allt mera, att vårt beroende av datorer ökar, att vi idag är åtskilligt professionellare inom ADB-säkerhetsområdet men att väldigt mycket finns att göra för att utveckla och införa nya metoder m m. Vi vet också att det finns gränser för hur snabbt inställningen till en fråga som denna kan ändras. Det tar många år att åstadkomma en attitydförändring.

6.1.3 Metodutveckling

Sårbarhetsproblemen kan av naturliga skäl inte slutgiltigt lösas vare sig metodologiskt eller praktiskt. Dessutom torde de växa i betydelse under de kommande åren till följd av den fortgående snabba datoriseringen.

Det är självklart att man inte kan slå sig till ro med hittills uppnådda resultat hur betydelsefulla de än må vara. Vårt beroende av ADB fortsätter att öka. ADB-miljön är dynamisk och metoder och hjälpmedel blir snart föråldrade. Nya problem, nya risker och hot dyker upp. Metod- och produktutveckling på ADB-säkerhetsområdet är i dag lika nödvändig som någonsin tidigare.

6.2 Slutsatser och förslag

I slutrapportens avsnitt 2 – 5 har SÅRB redogjort för det utvecklingsarbete som beredningen bedrivit. Projektredogörelserna i avsnitt 5 har var och en avslutats med de förslag och synpunkter i stort och smått som projekten i sig

och erfarenheterna av projektarbetet har givit. De viktigaste av dessa sammanfattas här.

6.2.1 Kunskap och metoder

Begreppsapparat. Den i ADB-säkerhet och sårbarhet hittills tillämpade begreppsapparaten är föråldrad och bör revideras. Särskilt är det nödvändigt att vidga och komplettera den hittills tillämpade, huvudsakligen på skyddsåtgärder inriktade terminologin. Bl a bör det ökade intresset för och kunskapen om sårbarhetsanalys beaktas vid en översyn av begreppsapparaten.

Primitiva metoder. Tillgängliga säkerhetsmetoder är i flera avseenden för primitiva. Det är tveksamt om metoderna kan ge ett godtagbart skydd av data som skall skyddas enligt sekretesslagen och datalagen. Saknar man godtagbara skyddsmetoder måste man införa eller upprätthålla restriktioner i teknikanvändningen.

System som i hög grad utnyttjar datakommunikation kräver särskild observans. Kryptering av överförd information utnyttjas idag i anmärkningsvärt liten omfattning. Behörigheten att få tillgång till data är ofta omfattande. De tekniska systemen för behörighetskontroll kringgås dessutom så att kontrollen i praktisk hantering blir undermålig. Tar man också hänsyn till att televerkets nät ger goda möjligheter till obehörig avlyssning blir den uppenbara slutsatsen, att datakommunikation endast bör användas för överföring av öppen eller – i krypterad form – tämligen okänslig information. Till detta kommer de publika nätens brister i fråga om driftsäkerhet. Detta är oroande mot bakgrund av den starka expansion som nu pågår inom datakommunikationsområdet.

Databrott är ett allvarligt riskområde där det finns utredningsmaterial från RPS och BRÅ samt från utlandet. Till skillnad från andra händelser av sårbarhetsnatur begås databrott högst medvetet. Det är viktigt att öka företagens och myndigheternas kunskaper om databrott och möjliga åtgärder.

Systemutveckling och systemkomplexitet. En viktig iakttagelse är att säkerhetsaspekterna fortlöpande måste ingå i systemutvecklingsprocessen. Redan tidigt under systemplaneringen skall säkerhetskraven bedömas och kalkyleras. Den hittillsvarande utvecklingen kännetecknas i hög grad av successiva, oplanerade ambitionshöjningar. Risken är då stor, att just säkerhetsaspekterna blir otillräckligt behandlade. Även om de blir beaktade kan det modifierade systemet visa sig vara mera svåröverskådligt än det ursprungliga och systemunderhållet alltför personberoende. Flertalet existerande system har genomgått en process med inslag av sådana förändringar. Komplexitets- och datakvalitetsfrågorna bör enligt SÅRB:s mening bli föremål för ytterligare utredning och forskning.

6.2.2 Utveckling och nya förutsättningar

Offentlighetsprincipens praktiska tillämpning har gett upphov till sårbarhetsdiskussioner. Det finns skäl som talar för att rätten till storskaliga uttag och bearbetningar av de statliga databaserna borde begränsas. Denna fråga

ligger f n hos Data- och offentlighetskommittén för utredning.

Erinringar mot myndigheternas utlämnande av inhämtad företagsinformation har också förekommit. När det gäller konkurrenskänsliga uppgifter visar SÅRB:s utredning att företagen ibland lämnar ofullständiga uppgifter. SÅRB kan inte bedöma om nyttan av ett ofullständigt register uppväger kostnaderna för registerhanteringen men vill peka på att man med dessa förutsättningar måste räkna med bristande kvalitet hos registret. Det finns enligt SÅRB:s mening anledning att överväga en större restriktivitet i spridningen av uppgifter, för vilka sekretess gäller. Tveksamt är om en behörighet som tilldelas tusentals tjänstemän att via terminal få tillgång till hemliga uppgifter verkligen är förenlig med sekretesslagens syften.

I SÅRB:s direktiv förs ett resonemang om vikten av att sårbarhetsaspekterna kommer upp till prövning inför generationsskifte av datorer och databehandlingssystem. Det är vid dessa generationsskiften som man enligt direktiven "kan och bör tillvarata den tekniska utveckling som möjliggör decentraliserade och mindre sårbara lösningar". Enligt SÅRB:s mening innebär decentralisering en sådan möjlighet och ett sätt att minska antalet behöriga högst väsentligt. En systemlösning som i princip baseras på centralt referensregister med öppet innehåll och lokalt fördelade databaser omfattande även sekretessbelagda data skulle sannolikt i många fall innebära väsentliga fördelar från säkerhetssynpunkt utan att effektiviteten blir mer än marginellt reducerad. Lösningar av den antydda typen diskuteras f n särskilt inom sjukvården. SÅRB har inte i något praktiskt exempel fått tillfälle att studera detta viktiga avvägningsproblem.

Ökat användarinflytande. I SÅRB:s tilläggsdirektiv sägs bl a att "Det är önskvärt att datoranvändarna i samhället gemensamt kan påverka bl a maskin- och programvaruleverantörer så att säkerheten så långt möjligt kan byggas in i utrustning och program och inte behöver kompletteras genom särskilda åtgärder i efterhand".

Det finns enligt SÅRB:s mening starka skäl att stödja en strävan efter ökad kompetens och inflytande hos användarna av datorer och datatjänster. Genom samverkan i branschorganisationer och intresseföreningar ges möjlighet att med mera kraft och kompetens föra fram krav och önskemål till dem som levererar datorer och programvara. Ett exempel på detta är projektet Kravspecifikation BKS där SIG-SEC med SÅRB bakom ryggen kan gå ut till BKS-leverantörer och med kraft kräva gehör för sina krav.

Oumbärlig databehandling i kris och krig. Förberedelse för kris och krig måste bygga på genomtänkta direktiv från statsmakterna till berörda myndigheter och företag i fråga om deras uppgifter i kris respektive krig. Här råder f n stora brister, samtidigt som det är uppenbart, att många för samhället vitala verksamheter inte längre kan utföras utan datorstöd. Detta gäller inte bara krigsmakten utan också näringslivet och – fast sannolikt i mindre mån – den offentliga förvaltningen utanför totalförsvaret.

SÅRB instämmer i FRI:s förslag (FRI 1985-10-01, Dnr 0640(48):001, Försvarets rationaliseringsplan 1985) att en kartläggning och analys av de olika samhällsfunktionernas beroende av datorstöd snarast påbörjas som en första åtgärd.

Även andra myndigheter och institutioner har gett uttryck för likartade synpunkter. 1978 års försvarskommitté har i sitt slutbetänkande (Ds Fö

1981:14) uttalat följande i fråga om programmet Ledning och samordning "Kommittén vill – – – framhålla betydelsen av att pågående studier av datorberoendet och möjligheterna att vidta åtgärder för att nödvändig datordrift skall kunna pågå under kriser och krig fortsätter. Det är därvid enligt kommitténs mening nödvändigt att i första hand kartlägga vilka system som måste vara i drift under kriser och krig".

Det går enligt SÅRB:s mening inte att konkret belysa samhällets beroende av ADB i kris- och krigssituationer utan vetskap om vilka funktioner/system som är oumbärliga och vilka vi kan tänka oss att avstå ifrån.

Minskat utlandsberoende. I avsnittet 5.2 Utlandsberoende har SÅRB diskuterat ett antal åtgärder som skulle bidra till att minska det allvarliga utlandsberoendet. SÅRB föreslår att bl a följande övervägs. Att staten stimulerar till en ökad andel s k tredjepartservice, att särskilda krav ställs vid upphandling på underhållsplanering och underhållsmässighet, insatser för att stimulera standardisering och lagerhållning av komponenter samt en översyn av mobiliseringsplaneringen.

Myndigheternas sårbarhet. De statsmyndigheter som är av särskild betydelse för totalförsvaret bör enligt SÅRB:s mening åläggas att *dels* analysera sårbarheten i sin datorbaserade verksamhet med SBA eller annan likvärdig metod, *dels* utarbeta plan för hur myndigheten skall fullgöra sina uppgifter vid bortfall av datorkraften

6.2.3 Sårbarheten och framtiden

Överblick och kontroll. I SÅRB:s direktiv sägs att ansvaret för effekterna av sårbarheten ofta faller utanför den särskilda myndighetens eller det särskilda företagets ansvar eller möjligheter att vidta åtgärder. Det är därför angeläget att samhället får överblick.

SÅRB:s erfarenheter bl a från projektet Offentlighetsprincipen, ADB och sårbarhet och inte minst från Postens transportstyrningssystem, PTS bekräftar att denna överblick är nödvändig om man vill få kontroll över sårbarheten och möjlighet att reducera den.

Samarbete om gemensamma problem. I SÅRB:s direktiv sägs att "Sårbarheten bör kunna minskas genom åtgärder som på eget initiativ kan vidtas inom en offentlig eller privat organisation. Av SÅRK:s betänkanden och remissyttranden framgår emellertid att åtgärder för att begränsa sårbarheten alltför ofta åsidosatts. Skälen härtill är bl a att kompetensen på detta område är begränsad och dessutom splittrad på olika funktioner i samhället". Det är även enligt SÅRB:s mening alltjämt viktigt att inte splittra de resurser som idag arbetar med sårbarhetsproblemen. Det är inte så att det är en särskild sorts hot som riktas mot totalförsvaret och en annan mot näringslivet och andra civila funktioner. Samma typer av hot finns över hela skalan av dataanvändare om än kanske av skilda skäl och vid olika tillfällen. Varje uppdelning av bevaknings- och utvecklingsarbetet – i en statlig och en privat del, med avseende på avsiktliga, brottsliga handlingar respektive oavsiktliga felhandlingar, samhällets respektive det enskilda företagets sårbarhet, osv är därför godtycklig och medför försämrad överblick, dubbelarbete och resursslöseri.

Sårbarhetsorgan. Den fortgående datoriseringen har, som SÅRB:s

utredningar klart visar stor inverkan på samhällets sårbarhet. Medvetandet härom ökar i takt med att säkerhets/sårbarhetsproblemen blir bättre belysta. För många myndigheter, företag och organisationer har SÅRB inneburit en möjlighet att få till stånd en diskussion av problem, som gått utanför ramen för den enskilda institutionens kompetens. Ett första led i diskussionerna har helt enkelt varit att konkretisera problemen.

De motiv som 1981 anfördes för bildandet av SÅRB äger fortfarande giltighet. Kompetensen är alltjämt mycket begränsad och dessutom splittrad på olika funktioner i samhället. Behovet för dataanvändarna att gå samman för att stärka sin ställning och ge tyngd åt sina krav gentemot starka leverantörskategorier är minst lika stort nu som för fem år sedan.

Enligt SÅRB:s mening talar allt för att samhället även framledes bör förfoga över ett organ som kan svara för allmän överblick och kraftsamling inom sårbarhetsområdet så som SÅRB hittills gjort.

Reservation

av ledamöterna *Göran Axelsson* och *Per Svenonius*

1 Inledande synpunkter

Sårbarhetsberdningen (SÅRB) har haft ett tidsbegränsat uppdrag och har verkat sedan sommaren 1981. Övervägande delen av verksamheten har skett i olika arbetsgrupper med representanter för statliga myndigheter, kommuner, landsting och företag eller genom anlitande av olika experter. I båda fallen har rapporter tagits fram som efter presentation och diskussion i själva beredningen har godkänts för publicering. Därvid har arbetsgruppen eller de anlitade experterna svarat för rapportens innehåll, efter hänsynstagande till de synpunkter som beredningen gett.

I ett mindre antal fall, t ex SÅRB:s handlingsplan (Ds Fö 1981:17), betänkandet Undanförsel och förstöring av ADB-register (Ds Fö 1983:8) samt rapporten "ADB i kris och krig" (den senare togs fram enligt tilläggsdirektiven för att överlämnas till försvarskommittén) har själva beredningen svarat för innehållet i rapporten eller betänkandet.

När SÅRB skulle avsluta sitt arbete till utgången av 1985 och utarbeta en slutrapport har tiden varit knapp för beredningen att gå igenom och ena sig om texterna. Dessa har behandlat en lång rad sakfrågor med anknytning till SÅRB:s handlingsplan. I kapitel 5 redovisas 16 olika frågor. Blandningen av frågor i detta kapitel om:

- extern miljö för ADB-verksamheten (fredstid, kris, krig)
- beroendet från utlandet
- utredningsmetoder som t ex SBA-metoden och kravspecifikation för behörighetskontrollsystem
- händelser av typen katastrofer, röjande signaler
- personfrågor
- åtgärder för att främja säkerheten som utbildning, kryptering,
- ADB-systemens tillstånd som t ex komplexitet
- teknik- eller användningsområden som t ex datakommunikation
- samhällsområden som t ex industrin och offentliga register

gör det svårt för läsaren att analytiskt förstå och värdera säkerhetsområdet. Inte förrän i avsnitt 5.16.2 finns en ansats att förklara ADB-säkerhetens begreppsapparat.

Den begränsade tillgängliga tiden har enligt vår mening inte medgett en mera kraftfull omredigering och anpassning av textmassan, baserat på en stringent begreppsapparat.

Vi vill varmt understryka det som SÅRB anför i avsnitt 5.16.3 att "Begreppsapparaten är enligt SÅRB:s mening mogen för översyn och revision".

Som ett steg i denna riktning vill vi peka på tre artskilda aspekter på sårbarhet.

Teknisk sårbarhet

Varje enskild systemägare ställs i sin ADB-säkerhetsplanering inför bedömningar av en mängd riskfaktorer. Vi anser det naturligt att förutsätta att varje systemägare av egenintresse utformar sitt säkerhetssystem så att ADB-säkerheten blir så god som möjligt med beaktande av gällande lagar (om integritet, sekretess, rättssäkerhet, databrott osv), god affärssed och annan praxis. I en sådan bedömning måste helt naturligt också ingå beroendeförhållanden gentemot andra system. Man skall kunna utgå från att varje system som tagits eller tas i drift, är utrustat med de säkerhetsfunktioner, som systemägaren på objektiva grunder kan finna motiverade. Kvarvarande risker (bl a katastrofrisker) måste man på samma grund förutsätta att systemägaren är beredd att ta de fulla konsekvenserna av om olyckan är framme, i medvetande om att säkerhetssystemet inte längre ger erforderligt skydd om katastrofen inträffar.

En säkerhetsbedömning av denna art skall rimligtvis alltid vara genomförd innan en systemägare beslutar att införa ett nytt system. Om den inte genomförs får detta uppfattas som ett ytligt ställningstagande till att katastrofrisker inte föreligger. Ett system som från början uppfyller alla säkerhetskrav, kan genom stegvisa utvidgningar nå en sådan kritisk punkt, att det inte tål ytterligare utökning. I princip skall därför varje systemförändring ur säkerhetssynpunkt prövas som om det vore ett nytt system. Om sårbarheten befinns vara oacceptabel skall det nya systemet inte införas.

Lagar, avtal och liknande

Gällande lagar, god affärssed och annan praxis handlar om regler, som i princip är allmängiltiga och som pålägger eller befriar systemägaren visst ansvar. Dessa regler utgör en viktig grundval för värdering av en systemägares ansvar vid katastrof.

Regler av denna art uttrycker samhälls-, sektor-, bransch- eller företagsövergripande krav eller utfästelser och kan inte ensidigt ändras av en enstaka systemägare.

Samhällets stabilitet

Man kan också identifiera ett ännu mer övergripande samhällskrav, värnet om samhällets stabilitet. Till detta sårbarhetsområde hör sådana störningar som samtidigt drabbar flera viktiga samhällssystem och ofta inte speciellt riktar sig mot ADB. Hit hör naturligtvis förhållanden vid beredskap och krig, men svåra problem kan uppträda även under fred, exempelvis handelshinder på det internationella området, katastrofer avseende elförsörjning och telekommunikationer på det inhemska. I sådana frågor måste statsmakterna

ständigt vara observanta och vid behov vidta åtgärder i stabilitetsfrämjande syfte.

Ett av problemen med den korta tiden för att utarbeta rapporten är att det finns svepande och långtgående formuleringar på sina håll i rapporten. Två fall behandlas i det följande.

2 Ang 5.6 om Datakommunikation

I rubr avsnitt 5.6 ges en innehållsförteckning till en ännu ej levererad rapport från televerket om säkerhet i datakommunikation. SÅRb konstaterar sedan i avsnitt 5.6.4 att "Risken för avlyssning av eller eljest känsliga data över Televerkets nät bör inte göra det utan att utnyttja kryptering." Enligt vår mening är denna utsaga illa underbyggd och inte korrekt med sin svepande formulering.

Vi vill peka på att SÅRB egentligen diskuterar "möjligheten att avlyssna" och inte "risken för avlyssning". Begreppet risk torde innefatta en stor eller liten sannolikhet eller rimlighet att någon har för avsikt att avlyssna en viss förbindelse. Att SÅRB skulle ha möjlighet att bedöma en sådan sannolikhet finner vi uteslutet.

Vi instämmer emellertid i uppfattningen att sådana system som i hög grad utnyttjar datakommunikation kräver särskild observans. Kryptering av överförd information utnyttjas i anmärkningsvärt liten omfattning. Som skäl härför anförs ofta att kryptering är svårt och kostsamt. Emellertid har det varit relativt lätt att införa kryptering i bankomatsystemet. Det är på motsvarande sätt önskvärt att höja säkerheten och integritetsskyddet i framför allt större system med person- eller annan känslig, men formellt icke-hemligstämplad information. De tekniska kraven är inte höga. Kryptering skall endast syfta till att förhindra att information på avvägar onödigtvis uppvisas i klartext.

För sändning av hemlig information över telenätet bör efter risk- och kostnadsanalys ett mer kvalificerat krypteringsförfarande övervägas.

Såvitt vi kan förstå är "möjligheten att avlyssna" televerkets nät starkt påverkad av vilken del av nätet som avses. Den delen av nätet som går från abonnenten till närmaste "telestation" torde vara lättare att avlyssna och samtidigt därvid igenkänna en viss kommunikation än vad gäller nätdelar som ligger djupare in i nätet. Inom televerket uppges att fastighetsnät i ett hyreshus kan vara relativt lätta att avlyssna. Många andra delar av nätet kan teoretiskt också avlyssnas och enskilda abonnenter igenkännas om en angripare sätter in omfattande resurser och lyckas hålla på tillräckligt länge.

Vilken slutsats ska systemägaren dra av denna information (som för övrigt lämnas av televerket)?

Systemägaren får försöka bedöma

- vilka intressen det kan finnas för att avlyssna, alternativt förvanska den information systemägaren sänder på televerkets nät
- vilka hot om avlyssning dessa intressen kan medföra från eventuella angripares sida
- vilka resurser och vilken uthållighet eventuella angripare rimligen kan sätta in för att avlyssna

– vilken förlust systemägaren gör om de eventuella angriparna lyckas.

Blir slutsatsen av detta att systemägaren fortsätter med att utnyttja televerkets nät utan åtgärder, att denne överväger krypteringsåtgärder (som kan vara dyrbara och komplicerade), att denne överväger andra åtgärder eller att denne avstår från att utnyttja nätet? Ja, detta måste var och en bestämma.

3 Ang 5.14 om Offentlighetsprincipen, ADB och sårbarhet

En annan enligt vår mening svepande och vilseledande formulering finns i rubr. avsnitt 5.14. Där finns en passus om myndigheternas mycket omfattande uppgiftsinsamling. I avsnitt 5.14.4 sägs "I detta sammanhang ter det sig naturligt för SÅRB att peka på myndigheternas mycket omfattande uppgiftsinsamling. SÅRB anser att de möjligheter som modern ADB-teknik ger kan användas på ett sätt som äventyrar säkerheten. Avvägning mellan nyttan av insamlade uppgifter och riskerna därmed sker icke alltid." Sedan framhåller SÅRB att aktuell lagstiftning normalt inte innefattar restriktioner i myndigheternas rätt att insamla uppgifter.

Såvitt vi kan bedöma har SÅRB inget underlag för att hävda att någon myndighet i Sverige samlar in mera data från företag och enskilda än vad som erfordras för att enligt statsmakternas beslut eller intentioner fullgöra ålagda uppgifter.

Däremot instämmer vi i SÅRB:s slutsats att riktlinjer saknas för myndigheternas försäljning av uppgifter och att sådan försäljning bör regleras i författning.

4 Ang kap 6 Resultat och förslag

SÅRB har i kapitlet betonat värdet av att myndigheter, företag och organisationer samarbetar för att lösa säkerhetsproblem. Det instämmer vi i.

Vi inser att SÅRB i kapitel 6 bör redovisa en allmän bedömning av ADB-säkerhetsområdet, behandla ansvarsfrågor på området och med detta som utgångspunkt lämna förslag om vilka åtgärder som rimligen den enskilde systemägaren (myndigheten, företaget, organisationen) bör svara för resp vad som bör ankomma på samhället att svara för.

SÅRB har inte gjort det senare utan har i stället framhållit att "De motiv som 1981 anfördes för bildandet av SÅRB äger fortfarande giltighet" som om inget positivt hänt under fem år från säkerhetssynpunkt. SÅRB anser också att allt talar för "att samhället även framledes bör förfoga över ett organ som kan svara för den allmänna överblick och kraftsamling inom sårbarhetsområdet så som SÅRB hittills gjort."

Mot denna bakgrund vill vi anföra följande:

SÅRB:s arbete har visat att många företag, myndigheter och för den skull hela samhället är mycket sårbart ur ADB-synpunkt i *krig*, mera sårbart än vad många kanske tidigare trott. Detta har redovisats av SÅRB till försvarskommittén i rapporten ADB i kris och krig. Beroendet av ADB är mycket stort, förmågan att arbeta manuellt är begränsad och stora delar av industrin står stilla utan ADB-stöd. Vårt elberoende och effekterna av

störningar på elnäten ökar sårbarheten ytterligare. Det är mycket angeläget att försvarskommittén och försvarsmyndigheterna med kraft arbetar vidare med dessa sårbarhetsfrågor och utarbetar åtgärdsförslag.

I det följande behandlas sårbarheten *enbart i normal fredstid.*

Ansvarsfrågor

Den ansvarsmässiga principen måste vara att varje företag och myndighet ansvarar för med vilken säkerhet verksamheten bedrivs. Det ankommer på dem att besluta om vilka åtgärder som behöver vidtas, inkl att i företag överväga vilka försäkringar som behöver tas.

Allmän bedömning av säkerheten

I Sverige används ADB relativt mycket, både i företag och hos myndigheter. Vi har också tillgång till den senaste tekniken både för databehandling och kommunikation. Spridningen av datatekniken, det ökande antalet datautbildade specialister och användare bidrar till denna expansion. Enligt uppgifter från LKD finns det f n ca 700 000 bildskärmar i landet, enligt SCB:s rapport Folkets Datorvanor fanns det 1984 ca 785 000 dataanvändare och ca 154 000 datayrkesverksamma i Sverige.

Antalet större och särskilt allvarliga störningar på data- och kommunikationsområdet är emellertid mycket begränsat i Sverige. Det måste rimligen tolkas som att *säkerheten allmänt sett är god på detta område.* Det inträffar naturligen ett stort antal störningar av skilda slag i en så omfattande verksamhet men i företag och myndigheter finns i regel en medvetenhet och förmåga att hantera dessa, varför störningarna mycket sällan lett till allvarliga problem.

En i sårbarhetssammanhang ofta diskuterad störning, stoppet på Stockholms Fondbörs under en vecka beroende på dataproblem på Värdepapperscentralen är egentligen en exceptionell händelse. Stoppen i AXE-stationerna under andra halvåret 1985 är, liksom börsstoppet att betrakta som i och för sig allvarliga, men dock intrimningsproblem.

Det har inträffat allvarliga störningar i elförsörjningen som gett oss en inblick i hur sårbart vårt samhälle är, men dessa störningar kan rimligen inte hänföras till sårbarhet på området data/kommunikation.

Det finns dock anledning till oro för att stora datacentraler skulle kunna drabbas av utslagning beroende på en katastrof (en oavsiktlig händelse utanför företagets eller myndighetens kontroll). En löpande bevakning av säkerheten mot katastrofer är angelägen.

Delområden med behov av säkerhetshöjande åtgärder

På ett antal delområden finns det mer eller mindre allvarliga problem med säkerheten. De kan dessutom komma att växa om inte särskilda åtgärder genomförs.

SÅRB har i avsnitt 6.2.1 pekat på områden som

- tele- och datakommunikationsnäten
- databrott
- systemutveckling och systemkomplexitet

samt i avsnitt 6.2.2 pekat på områden som

- offentlighetsprincipens praktiska tillämpning (med försäljning av information)
- sekretesslagens tillämpning vid överföring av information
- minskat utlandsberoende
- myndigheternas sårbarhet

Vi kan instämma i att det behövs säkerhetshöjande åtgärder på dessa områden. Vi vill också peka på att frågan om handelsbegränsningar på data- och elektronikområdet är ett annat område där speciellt staten har att överväga åtgärder.

Statsmakternas åtgärder

Slutsatsen av detta är att behovet av ett allmänt sårbarhets- och säkerhetsarbete som avser problemnivån införande och drift av ADB-system i den fredstida användningen numera är mindre för statsmakterna än det varit under de senaste 10 åren, då SÅRK och SÅRB varit verksamma.

Samtidigt ger SÅRB:s rapporter regeringen incitament för att överväga insatser på speciella områden. Detta arbete kan kopplas till det ansvar som finns för dessa områden. Vidare kan regeringen överväga att få utvecklingen av samhällets sårbarhet i stort, på grund av *flera* faktorer som elektricitet, data- och kommunikationsteknik men kanske även som en följd av utlandsberoendet, bevakad och de väsentliga problemen konkretiserade.

Regeringen har den 16 januari 1986 beslutat bilda en statsrådsgrupp med uppgift att särskilt följa ADB-frågorna, däribland säkerhetsfrågorna. Statsrådsgruppen avses få biträde av en samrådsgrupp för sårbarhet på ADB-området med bred representation från landstingskommuner och det privata näringslivet.

Regeringen har samma dag uppdragit åt chefen för justitiedepartementet att bilda en sådan samrådsgrupp. Gruppens uppgift skall vara att på uppdrag av statsrådsgruppen för ADB-frågor, analysera sårbarhetsfrågor inom ADB-området samt lägga fram förslag till konkreta åtgärder för att minska sårbarheten.

Enligt vår mening är det då naturligt att samrådsgruppen koncentrerar sitt arbete på viktiga sårbarhetsfrågor på samhällsnivån, d v s på frågor som myndigheter, företag och organisationer, enskilt eller i samverkan inte har möjlighet att lösa och på frågor som direkt berör flera departement.

Åtgärder som systemägare bör genomföra

Vi anser att det är viktigt att företagens och myndigheternas verksamhet bedrivs med hög säkerhet. För att leva upp till sitt ansvar för säkerheten måste de mer eller mindre ständigt överväga nya åtgärder resp revidera befintliga. Detta är ett tekniskt, organisatoriskt och personellt arbete.

För företagen och myndigheterna kan det finnas ekonomiska, kunskapsmässiga och tekniska fördelar med att utveckla tekniska metoder och utredningstekniker samt genomföra en del utredningar och studier i *samverkan*. SÅRB:s och RDF:s arbete med SBA-metoden och olika

intressenters ekonomiska och arbetsmässiga satsningar på detta arbete visar att företag och myndigheter är beredda att betala för att sådana metoder tillhandahålls eller utvecklas.

Vi anser att ett tekniskt samarbete av angiven art är önskvärt även i framtiden. Det bör i allt väsentligt ankomma på vissa myndigheter med speciellt ansvar som statskontoret, FRI, televerket och STU, på organisationer som RDF, LKD, Svenska Samfundet för Informationsbehandling och Svenska Dataföreningen samt övriga speciellt intresserade företag och myndigheter att finna former för ett vidareutvecklat samarbete på detta område.

Det kan erinras om att regeringen har föreslagit riksdagen att statskontoret skall ha ett övergripande ansvar för säkerhetsfrågorna inom statsförvaltningen. Enligt regeringens förslag bör de metoder som utvecklas för att minska sårbarheten inom dataområdet för statsförvaltningen även kunna tillämpas inom samhället i övrigt. Riksdagen har bifallit dessa förslag.

Statskontoret – liksom många andra myndigheter – samarbetar redan idag med RDF. Det ligger nära till hands att tänka sig att gemensamma projekt inom säkerhetsområdet även framgent skulle kunna genomföras i RDF:s regi.

Systemägare samt organ som statskontoret har även anledning att enskilt eller i samverkan ägna sig åt löpande bevakning och problemkonkretisering på ADB-säkerhetsområdet, vilket kompletterar den överordnade bevakning av det svenska samhällets sårbarhet på ADB-området som samrådsgruppen kan komma att arbeta med.

Bilaga 1

Kommittédirektiv

Dir 1981:48

Information och rådgivning i frågor rörande säkerhet och sårbarhet på dataområdet

Dir 1981:48

Beslut vid regeringssammanträde 1981-07-23

T. f. chefen för försvarsdepartementet, statsrådet Söder, anför.

Enligt beslut av regeringen tillsattes våren 1977 sårbarhetskommittén (SÅRK Fö 1977:02) med uppgift att utreda sårbarheten hos det datoriserade samhället och att föreslå åtgärder för att minska denna.

Kommitténs kartläggning som redovisades i betänkanden år 1978 (Ds Fö 1978:4) och år 1979 (SOU 1979:93) ledde fram till den allmänna slutsatsen att sårbarheten är oacceptabelt hög i dagens "ADB-samhälle". Den fortgående utvecklingen leder även, enligt kommitténs uppfattning, till en allt högre sårbarhet i framtiden om inte motåtgärder vidtas. Denna bedömning gäller såväl för krigs- och beredskapssituationer som för förhållanden under fredstid.

Sårbarheten är enligt kommittén betingad av flera faktorer. De mest betydande är utlandsberoendet, koncentrationen, kommunikationerna, personalberoendet och de risker som hänger samman med vissa typer av registerinnehåll. Olika yttre angrepp möjliggörs eller underlättas av dessa sårbarhetsfaktorer.

Kommittén konstaterar också att beredskapen mot kriminella handlingar, missbruk för politiska syften och krigshandlingar många gånger är obefintlig eller i vart fall otillräcklig.

När det gäller möjligheten att komma till rätta med sårbarheten anser SÅRK att sårbarheten kan begränsas i redan existerande ADB-system. Nya system bör genom en sårbarhetsbedömning kunna byggas upp annorlunda än hittills har skett.

I syfte att uppnå detta mål föreslog SÅRK bl. a. en satsning på rådgivning och information men även viss lagstiftning för att få till stånd en sårbarhetsprövning av stora och viktiga ADB-system i första hand inom den offentliga sektorn.

Vid remissbehandlingen har SÅRK:s analys och principiella uppfattning fått starkt stöd. Med få undantag har remissinstanserna också instämt i

slutsatsen att sårbarheten är oacceptabelt hög och att snara motåtgärder är erforderliga.

När det gäller de åtgärder som kommittén föreslagit är uppfattningarna däremot mera delade. I fråga om behovet av lagstiftning och dess eventuella utformning finns det mycket skilda åsikter. I fråga om behovet av information och rådgivning är däremot samstämmigheten stor.

Datasårbarheten har uppmärksammats även av 1978 års försvarskommitté, som understryker att studierna av sårbarheten bör fortsätta. Det är enligt kommittén nödvändigt att kartlägga vilka system som måste vara i drift i kriser och krig.

Jag instämmer i sårbarhetskommitténs allmänna slutsats att sårbarheten i samhället är oacceptabelt hög på grund av den hittillsvarande datoriseringen. Motåtgärder bör därför vidtas. Denna uppfattning delas av flertalet remissinstanser. Sårbarheten bör kunna minskas genom åtgärder som på eget initiativ kan vidtas inom en offentlig eller privat organisation. Av SÅRK:s betänkanden och remissyttranden framgår emellertid att åtgärder för att begränsa sårbarheten alltför ofta åsidosatts. Skälen härtill är bl. a. att kompetensen på detta område är begränsad och dessutom splittrad på olika funktioner i samhället. Det har dessutom i praktiken varit mycket svårt för användare av *enskilda system* att se effekterna av dessa på *samhällets* sårbarhet.

Ofta faller sålunda ansvaret för effekterna av sårbarheten utanför den särskilda myndighetens eller det särskilda företagets ansvar eller möjligheter att vidta åtgärder. Det är därför angeläget att samhället får överblick och kan ta initiativ till åtgärder som syftar till ett mindre sårbart samhälle. Detta gagnar också vårt totalförsvar.

Av hänsyn till den blandade remissopinionen och till det ekonomiska läget som i allmänhet inte möjliggör några mera omfattande statliga insatser utan motsvarande omprioriteringar anser jag att man måste finna delvis andra former för att komma till rätta med sårbarheten än dem SÅRK föreslagit. Så långt möjligt bör detta ske på frivillig väg. Information och rådgivning måste därför bli ett väsentligt inslag. För detta liksom för nödvändig överblick bör samhället ta ansvar.

Beträffande stora eller på annat sätt viktiga system på den statliga sidan bör man emellertid finna sådana rutiner att en sårbarhetsprövning regelmässigt kommer till stånd som ett led i handläggningen av ärenden inför statsmakternas ställningstagande. Sårbarhet måste därvid självfallet vägas mot de andra aspekter som kan vara aktuella vid prövningen.

Mot denna bakgrund anser jag att en beredning bör tillkallas för att utarbeta en handlingsplan och en närmare precisering av vilka sårbarhetsfaktorer och sårbarhetsproblem som kräver särskild uppmärksamhet och åtgärder från samhällets sida. En sådan redogörelse bör färdigställas och

överlämnas till regeringen före årsskiftet 1981/82 för att kunna prövas i samband med 1982 års totalförsvarsproposition och den aviserade datapolitiska propositionen till våren 1982. I dessa sammanhang är det även naturligt att beredningens fortsatta verksamhet tas upp. I avvaktan på detta bör dock åtgärder vidtas för att minska sårbarheten.

Beredningen bör därför tills vidare även vara ett rådgivande organ med representation för berörda statliga myndigheter, kommunerna och näringslivet. Såsom flera tunga remissinstanser anfört kan ett sådant organ samla och söka nyttiggöra hittills gjorda erfarenheter. Beredningen skall målmedvetet och aktivt verka för en minskad sårbarhet. Härvid bör de säkerhetspolitiska konsekvenserna av olika åtgärder särskilt uppmärksammas.

I beredningens övriga uppgifter bör också ingå att 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.

Beredningen bör tills vidare även kunna svara för sådan information och rådgivning och verksamheten riktas till såväl den offentliga som den privata sektorn.

Enligt min mening är det viktigt att sårbarhetsaspekten kommer upp till prövning inför generationsskifte av datorer och databehandlingssystem. Av ekonomiska skäl kan det i många fall vara en omöjlighet att vidta lämpliga åtgärder vid andra tillfällen medan kostnaderna för åtgärderna i samband med ett generationsskifte kan bli små. Det är även vid dessa generationsskiften som man kan och bör tillvarata den tekniska utveckling som möjliggör decentraliserade och mindre sårbara lösningar.

En annan huvuduppgift som tills vidare bör åläggas beredningen är att fungera som remissinstans på sårbarhetsområdet. Främst gäller detta vid investeringar i stora datasystem på den statliga sidan. Det är väsentligt att sårbarhetsfrågorna blir beaktade innan statsmakterna fattar beslut om stora eller eljest viktiga ADB-system.

Myndigheter bör samråda med beredningen i frågor inom dataområdet som rör sårbarhet.

På många områden av betydelse för samhällets sårbarhet är kunskaperna fortfarande bristfälliga. Det gäller bl. a. ett sådant område som utlandsberoendet av datautrustning (hel- och halvfabrikat), komponenter samt programutrustning. Det gäller även de beroendeförhållanden som skapas genom att databehandling för ändamål i vårt land utförs i andra länder, bl. a. med utnyttjande av modern kommunikationsteknologi som exempelvis datanät och satellitkommunikation. Beredningen bör i dessa avseenden göra en fortsatt och fördjupad analys och bedöma behovet av ytterligare åtgärder. Bl. a. bör möjligheten att ersätta utslagen datorkapacitet belysas.

Överstyrelsen för ekonomiskt försvar svarar bl. a. för samordning av

beredskapsplanering av sådan informationsbehandling som kräver datorstöd, för planeringen av försörjningsberedskapen inom näringslivet, där databehandlingssystem utgör en viktig del samt för frågor rörande undanförsel och förstöring.

Beredningen bör samarbeta med överstyrelsen i frågor rörande sårbarhetsfaktorer inom överstyrelsens ansvarsområde.

Frågan om rutiner och lagstiftning för förstöring av personregister bör övervägas i samråd med datalagstiftningskommittén (Ju 1976:05).

Beredningen bör lägga grunden för en fortlöpande bevakning av sårbarhetsfrågorna och ta fram underlag till mer permanenta åtgärder.

Beredningen bör bedriva sitt arbete så att detta kan vara avslutat och utvärdering gjord senast den 1 juli 1984.

Beredningen bör ha en representation från berörda statliga myndigheter, från näringslivet samt från kommuner och landsting som svarar för stora och viktiga datasystem. Information om beredningens arbete bör i erforderlig omfattning ges till arbetsmarknadens parter.

Beredningens behov av utredningsresurser bör i första hand tillgodoses genom att utnyttja de resurser som finns inom berörda myndigheter såsom datainspektionen, datamaskincentralen för administrativ databehandling, försvarets rationaliseringsinstitut, försvarets datacentral, statskontoret och överstyrelsen för ekonomiskt försvar.

Beredningen bör nära samarbeta med dessa myndigheter samt med delegationen för datafrågor (B 1980:3).

Med hänvisning till vad jag nu har anfört hemställer jag att regeringen bemyndigar chefen för försvarsdepartementet

att tillkalla en beredning med högst 10 ledamöter för utredning av och för information och rådgivning i frågor rörande säkerhet och sårbarhet på dataområdet

att utse en av ledamöterna att vara ordförande,

att besluta om sakkunniga, experter, sekreterare och annat biträde åt beredningen.

Vidare hemställer jag att regeringen beslutar

att kostnaderna för beredningen skall belasta fjärde huvudtitelns kommittéanslag.

Regeringen ansluter sig till föredragandens överväganden och bifaller hennes hemställan.

(Försvarsdepartementet)

Bilaga 2

Kommittédirektiv

Dir 1984:29

Tilläggsdirektiv till sårbarhetsberedningen (Fö 1981:02)

Dir 1984:29

Beslut vid regeringssammanträde 1984-06-20

Chefen för försvarsdepartementet, statsrådet Thunborg anför.

Sårbarhetsberedningens uppgifter

Sårbarhetsberedningens (SÅRB) uppgifter är främst att precisera vilka sårbarhetsfaktorer och sårbarhetsproblem inom dataområdet som kräver särskild uppmärksamhet från samhällets sida (Dir 1981:48). Härutöver skall beredningen tills vidare vara ett organ för information och rådgivning och fungera som remissinstans inom sårbarhetsområdet, främst när det gäller stora statliga datasystem.

I direktiven anges att beredningens arbete bör vara avslutat senast den 1 juli 1984.

Beredningen arbetar efter en arbetsplan (Ds Fö 1981:17) från den 16 december 1981. Planen upptar ett stort antal projekt och arbetsområden av betydelse för samhällets sårbarhet.

Beredningen har i samarbete med bl.a. Riksdataförbundet, ett flertal statliga myndigheter, näringsliv och organisationer utarbetat en speciell metod för sårbarhetsanalys av datoriserade informationssystem, den s.k. SBA-metoden. En presentation av SBA-metoden har sänts ut till ett stort antal företag, kommuner, landstingskommuner och myndigheter. Detta ingår i den plan som beredningen arbetar efter för att utvärdera och vid behov förändra metoden.

Beredningen har i augusti 1983 överlämnat betänkandet (Ds Fö 1983:8) Undanförsel och förstöring av ADB-register. Betänkandet bereds f.n. inom regeringskansliet.

Enligt direktiven och arbetsplanen återstår alltjämt att redovisa ett omfattande utredningsarbete. I februari 1984 har SÅRB hemställt om att få förlängd utredningstid på grund av resursproblem.

Överväganden

Enligt min mening är det arbete som har utförts av SÅRB och sårbarhetskommittén (SÅRK, Dir 1977:56) av stor betydelse även för totalförsvaret. I de direktiv (Dir 1984:14) som i mars 1984 har getts till en ny försvarskommitté anges bl.a. att den skall lämna förslag till vilken säkerhet som skall eftersträvas inom ADB-området under kriser och i krig, ställt i relation till den säkerhet som finns redan i fred. I direktiven anges att försvarskommittén härvid skall utgå från underlag som regeringen kommer att ställa till dess förfogande, bl.a. från arbetet inom SÅRB.

I proposition 1983/84:100 (bil. 2 s. 11) anför chefen för civildepartementet att han anser det vara viktigt att bl.a. myndigheter och andra organ inom den offentliga sektorn bevakar sårbarhetsaspekterna och nämner därvid särskilt SBA-metoden. Stora delar av den offentliga sektorn kan komma att överväga att utnyttja SBA-metoden i sin verksamhet. Behov av olika skyddsåtgärder och nyttan av dessa får då vägas mot kostnaderna för åtgärderna och de nackdelar i övrigt som kan uppstå. I viss mån kan samma förhållande uppträda inom näringslivet. För samtliga berörda är frågan om säkerhet således förknippad med kostnader och effekter. För den statliga verksamheten skall frågan prövas i samband med budgetarbetet. Behovet av olika säkerhetsåtgärder och kostnaderna för dessa kan därmed vägas mot varandra i samband med regeringens m.fl. beslut om utveckling och anskaffning av ADB-system. Motsvarande överväganden bör enligt min mening göras även vid utveckling och anskaffning av ADB-stöd inom andra samhällssektorer. Emellertid är det också klarlagt att sårbarhetsaspekterna inte kan behandlas isolerade utan måste vägas in i en totalbild, när bl.a. utveckling eller anskaffning av informationssystem övervägs.

Säkerhetskraven inom ADB-området kan tillgodoses med olika typer av tekniska och administrativa åtgärder. Det är önskvärt att datoranvändarna i samhället gemensamt kan påverka bl.a. maskin- och programvaruleverantörer så att säkerheten så långt möjligt kan byggas in i utrustning och program och inte behöver kompletteras genom särskilda åtgärder i efterhand.

Ett omfattande utrednings- och utvecklingsarbete inom området har genomförts såväl inom den offentliga sektorn som i näringslivet. Jag anser att det är mycket angeläget att de erfarenheter och det breda kunnande inom området sårbarhet/säkerhet som SÅRB besitter tas till vara för att dels redovisa en översikt av genomfört utrednings- och utvecklingsarbete inom området ADB-säkerhet, dels analysera användbarheten av det tillgängliga materialet. I de fall där beredningen finner att ett kompletterande arbete bör utföras skall SÅRB föreslå åtgärder för att komma till rätta med problemen.

SÅRB bör i första hand redovisa resultaten av beredningens handlingsplan

och då främst SBA-metoden. I andra hand bör SÅRB inventera hittillsvarande arbete inom området ADB-säkerhet, analysera materialet och föreslå eventuella åtgärder. Härutöver kvarstår uppgifterna att svara för information, ge råd samt vara remissorgan i sårbarhetsfrågor inom ADB-området. Dessa senare uppgifter bör emellertid få stå tillbaka för de två första i de fall prioriteringar måste göras.

Beredningen bör utökas med representanter från näringslivet för att den skall få ett tillräckligt brett erfarenhetsunderlag för sitt arbete.

Förslag

Mot denna bakgrund föreslår jag att sårbarhetsberedningen ges tilläggsdirektiv att inventera hittillsvarande arbete inom området ADB-säkerhet, analysera användbarheten av detta material samt att i samverkan med främst statskontoret föreslå förbättringar och kompletteringar i de fall beredningen anser det vara motiverat.

Jag föreslår vidare att SÅRB:s arbete med information, rådgivning och remissverksamhet främst skall riktas mot de myndigheter och företag som har störst betydelse för den civila delen av totalförsvaret.

I fråga om tidsförhållanden bör följande gälla:

- SÅRB:s arbete med SBA-metoden skall redovisas under år 1984.
- SÅRB skall senast den 2 maj 1985 till regeringen redovisa de erfarenheter från sitt arbete som kan utnyttjas som ett av de underlag som regeringen ställer till försvarskommitténs förfogande.
- SÅRB skall i sin planering utgå från att beredningens arbete skall avslutas under år 1985.

Hemställan

Jag hemställer att regeringen lämnar tilläggsdirektiv till sårbarhetsberedningen i enlighet med vad jag nu har anfört samt bemyndigar chefen för försvarsdepartementet att utöka beredningen till högst 12 ledamöter.

Beslut

Regeringen ansluter sig till föredragandens överväganden och bifaller hans hemställan.

(Försvarsdepartementet)

Bilaga 3

Rapporter från SÅRB

- Sårbarhetsberedningens (SÅRB) handlingsplan (Ds Fö 1981:17).
- Informationsskrift från SÅRB/Riksdataförbundet (RDF) ADB-säkerhet och sårbarhet.
- Information om SBA.
  - Bakom datorernas rubriker
  - SBA information
  - SBA Security By Analysis (Engelsk version av SBA information)
  - SBA prislista och materialbeställning(SBA-metoden omfattar 10 st skrifter. Dessutom finns handledning, video, stordia, blanketter. Beställs hos Utbildningsproduktion AB.)SBA-metoden omfattar följande delar:
    SBA-start
    SBA-Beroende
    SBA-System
    SBA-Scenario
    SBA-Plan
    SBA-Rapport
    SBA-Projekt
    SBA-Utveckling
    SBA-Nyckelpersonal
    SBA-Revision
    Varje del kan även köpas separat.
- Undanförsel och förstöring av ADB-register (Ds Fö 1983:8).
- Läckande datorer, en information om Rös (Röjande signaler). Informationsskrift från SÅRB/Brotsförebyggande rådet. (BRÅ).
- Rapport 1983:12 Nyckelpersonal inom datordrift.Om hur man kan minska beroendet av nyckelpersoner.
- Rapport 1984:1 Praktisk katastrofplanering – Val av reservdriftalternativ.
- Rapport 1984:2 Aktuella projekt i SÅRB.Projektförteckning från 1984.
- Rapport 1984:3 Uppringda datorer. Om problemen med hackers och hur man undviker dem.

- Rapport 1984:4 Offentlighetsprincipen, ADB och försvarssekretess.
- Rapport 1985:1 ADB i kris och krig. Rapport till försvarskommittén.
- Rapport 1985:2 Personal och säkerhet. Hur man rekryterar, organiserar och administrerar ADB-personal.
- Rapport 1985:3 ADB-säkerhet och sårbarhet. Ett kompendium. Kompendium avsett för 3-4 timmars lektion om ADB-säkerhet och sårbarhet. (Se även Datasäkerhet – en svensk tiger.)
- Den sårbara Datorn. Broschyr för skolor och utbildningsanstalter. Kortfattad orientering om ADB-säkerhet och sårbarhet.
- Den sårbara Datorn. Affisch. Samma innehåll som broschyren.
- Rapport 1985:4 Systemkomplexitet och sårbarhet.
- Rapport 1985:5 Säkerhetskrav på datorer och operativsystem. SÅRB/SIG-SEC
- Rapport 1985:6 Kassaskåpssäker sekretess och ADB.
- Kryptering i ADB-system. Praktisk hjälpreda för beslutsfattare och systemerare. SIS tekniska rapport 312. Kan beställas från Riksdataförbundet eller Sveriges Standardiseringskommission, SIS.
- Datakommunikationernas sårbarhet. Utges av Televerket i samråd med SÅRB i början av 1986.
- Datasäkerhet – en svensk tiger. Kompendium – samma som Rapport 1985:3 men med handledning, bilder etc. Utges av Utbildningsproduktion AB och Riksdataförbundet i början av 1986.

Bilaga 4

"Undersökning ang Värdepapperscentralen VPC Aktiebolags dataproblem, leveransförseningar m m".

(Bankinspektionens rapport 1983-12-15.)

Utdrag

– – – –

4.2.4 VPC-systemets sårbarhet och frågor om ADB-säkerhet

VPC-systemet är, i likhet med bankernas elektroniska betalningssystem ett sådant funktionellt känsligt datasystem som med hänsyn till framför allt konsekvenserna av driftsavbrott kräver särskild uppmärksamhet på ADB-säkerhetsfrågor. VPC åtnjuter en monopolställning inom det verksamhetsfält bolaget arbetar på. Att VPC med sin centrala betydelse för den svenska aktiehandeln löser sina uppgifter på ett tillfredsställande sätt är därför av allmänt intresse. Detta markeras av att staten gått in som hälftenägare i VPC.

Mot denna bakgrund ligger det i sakens natur att VPC måste ha personella och tekniska resurser som kan möta också oväntade störningar och volymökningar i sin verksamhet. De problem som VPC haft att brottas med under de senaste åren utgör en illustration till sårbarheten i VPC:s verksamhet. Arbetsgruppen anser att erforderliga ADB-säkerhetsåtgärder för att lösa problemen ej motsvarat de krav som VPC:s känsliga position ger anledning att ställa. VPC:s ledning och styrelse kan inte undgå viss kritik härför.

Det torde vara väl bekant att bl a bankerna aktivt agerat i frågor om s k katastrofplanering och samtliga banker har träffat en principöverenskommelse om hjälp till bank som drabbas av längre driftsavbrott. I detta hänseende är förhållandena otillfredsställande hos VPC. I samarbetet med ICL har VPC hittills inte lyckats uppnå någon godtagbar lösning beträffande reservdatoranläggning. En beredskapsplan krävs vidare som bl a klargör frågor om vilka servicefunktioner som efter längre produktionsstopp skall prioriteras i olika faser under en period av återgång till normal verksamhet.

Denna plan är en fråga på styrelsenivå. En genomgång både under 1981 och 1982 av driftkontroller hos VPC har genomförts av utomstående revisions- och ADB-expertis. Redovisade iakttagelser i PM, vilka ej föredragits eller anmälts vid styrelsesammanträde, ger klart besked om att säkerheten eftersatts inom den löpande datordriften. Arbetsgruppen har under sin kartläggning av omregistreringsrutinen för sin del konstaterat brister i systemdokumentation. En väsentlig del av ADB-säkerheten är att bygga upp och underhålla systemöversikter, utdataspecifikationer, programbeskrivningar etc, så att ett beroende inte uppstår till s k nyckelpersoner med exklusiv kunskap om datasystemets funktionssätt.

Till ADB-säkerhet hör också sådana åtgärder som syftar till att skydda VPC, med sina stora och till innehållet känsliga person- och värdepappersregister, mot såväl oavsiktliga fel i redovisningen som risker för oegentligheter. Behörighetsregler är så väsentliga att de bör fastställas på styrelse- eller ledningsnivå. Arbetsgruppen har som redovisas i denna rapport konstaterat att kontrollen inom omregistreringsrutinen är otillfredsställande. Personalresurserna för systemutveckling och systemunderhåll har varit för små och många skisserade projekt med säkerhetshöjande inriktning har fått anstå. En probleminventering har nu påbörjats inom VPC, varvid bl a en systemrevision i syfte att analysera och förbättra säkerheten ingår. Arbetsgruppen har också erfarit att en utrednings- och kontrollgrupp tillsatts. VPC har emellertid enligt arbetsgruppens mening även ett starkt behov av en internrevisionsfunktion, som i nära kontakt med produktionen kan granska den interna kontrollen, följa ADB-projekt under utveckling m m.

Arbetsgruppen utgår från att full insikt om sårbarhetsproblemets vidd har vunnits hos VPC efter "datorhaveriet". I den organisationsöversyn som pågår inom VPC har föreslagits att en sårbarhets- och säkerhetsfunktion inrättas. Arbetsgruppen anser att detta är ett nödvändigt steg. Här kan säkerhetschefsfunktionen hos bankerna tjäna som mönster. En metod för strukturering av sårbarhetsfrågorna, den s k SBA-metoden, har nyligen presenterats av den s k sårbarhetsberedningen, Riksdataförbundet m fl och kan rekommenderas.

– – –

Säkerhetsåtgärder vidtagna hos VPC 1983-1985

Värdepapperscentralen VPC AB har vidtagit ett antal säkerhetshöjande åtgärder. VPC har till SÅRB PM 1985-12-16 lämnat följande redovisning.

"Genom en massiv insats av resurser såväl personella som maskinella, stabiliserades ADB-produktionen hos VPC under 1983. Härigenom upprepades inte de längre förseningar som under sommaren 1983 medförde problem för VPC och fondhandeln. Därefter har inom VPC vidtagits en mängd åtgärder för att öka säkerheten i ADB-systemet.

Vid en omorganisation av VPC i slutet av 1983 knöts ADB-driften närmare användaravdelningarna genom att ADB-driftavdelningen då flyttades till produktionssektionen. På ADB-driftavdelningen förstärktes funktionen för teknisk support

och dessutom infördes en särskild planeringsfunktion. Genom utbildningsåtgärder höjdes kunnandet om det nya operativsystemet bland operatörer och personal för teknisk support.

Vitala datorfunktioner har dubblerats. Sålunda finns nu två processorer som var för sig kan utföra erforderliga ADB-bearbetningar men som normalt är dualkopplade. Skivminneskontrollenheter och kommunikationsdatorer är också dubblerade. Även skivminnesutrymme finns nu i så stor omfattning att körningarna kan genomföras även om en eller ett par enheter inte fungerar.

För att ytterligare säkra ADB-driften tog VPC fram ett produktionsplaneringssystem som minimerat operatörsingripanden och avsevärt ökat säkerheten i datorbearbetningarna. I samband med att planeringssystemet togs i drift gjordes också en omfattande genomgång av säkerhetsrutiner och driftrutiner i ADB-produktionen.

Eftersom stora värden överförs via ADB-media från VPC till olika mottagare finns det anledning att åstadkomma så hög säkerhet som möjligt vad gäller dataskyddet. VPC inför därför för närvarande rutiner med elektroniskt sigill på vissa magnetband.

Under 1984 gjordes en total övergripande översyn av säkerheten inom företaget. Därvid föreslogs bl a att en katastrofplan skulle utarbetas. En projektgrupp har under 1985 tagit fram en katastrofhandbok för VPC, samt träffat avtal om back-up-dator och back-up-lokaler som kan användas vid en eventuell katastrof. Produktionstester har genomförts på back-up-datorn. Den datorkapacitet som står till VPC:s förfogande vid en katastrof är begränsad och medger endast att de viktigaste rutinerna kan genomföras. Därför har datorleverantören förbundit sig att inom 10 dagar kunna leverera en ny datoranläggning av samma storlek och omfattning som VPC förfogar över vid katastroftillfället. För att säkerställa att denna dator kan placeras i en lämplig lokal har VPC träffat särsklit avtal om back-up-lokal.

VPC har under 1985 flyttat till nya ändamålsenliga lokaler. Datorhall och efterbehandlingsutrymmen har utformats så att driftmiljön underlättar personalens arbete, vilket medverkar till en säker och effektiv datordrift. Reservkraft, såväl batterier som dieselgeneratorer, har installerats. VPC arbetar vidare långsiktigt på ett nytt kontobaserat värdepapperssystem som när det genomförts kommer att medföra en höjd datakvalitet i systemet."

Bilaga 5

Sårbarhetsberedningen (Fö 1981:02) (SÅRB)

Tillkallade enligt regeringens bemyndiganden den 23 juli 1981 och den 20 juni 1984 för utredning av och för information och rådgivning i frågor rörande säkerhet och sårbarhet på dataområdet:

Ordförande:
Eriksson, Allan, kansliråd

Ledamöter:
Andersson, Benny, sektionschef (fr.o.m. den 9 december 1982)
Axelsson, Göran, kanslichef
Carlsson, Ulf, verkst. direktör
Essén, Johan, ADB-säkerhetschef (fr.o.m. den 30 augusti 1984)
Freese, Jan H:son, generaldirektör
Hertz, Olof, avdelningsdirektör (t.o.m. den 31 december 1982)
Holmertz, Göran, byrådirektör (fr.o.m. den 1 januari 1983 t.o.m. den 20 oktober 1985)
Holmström, Bo, avdelningschef (t.o.m. den 5 april 1983)
Hoving, Per, fil.kand. (fr.o.m. den 30 augusti 1984)
Jonsson, Göte, direktör (t.o.m. den 8 december 1982)
Lundberg, Bruno, utredningschef
Lundberg, Orvar, överste (fr.o.m. den 6 april 1983)
Nilsson, Bengt-Erik, byråchef (fr.o.m. den 21 oktober 1985)
Svenonius, Per, avdelningschef
Vinge, Per-Gunnar, direktör

Sakkunnig:
Engqvist, Mikael, departementssekreterare (fr.o.m. den 25 aptil 1983 t.o.m. den 15 oktober 1985)

Experter:
Hedqvist, Jan, byråsekreterare (fr.o.m. den 2 oktober 1984 t.o.m. den 15 oktober 1985)
Lindgren, Lars, departementssekreterare (fr.o.m. den 17 september 1984)
Nilsson, Torbjörn, rationaliseringschef (fr.o.m. den 17 september 1984)
Sundvall, Mats, byråsekreterare (fr.o.m. den 30 augusti 1984 t.o.m. den 15 oktober 1985)

Huvudsekreterare:
Wrede, Rabbe, avdelningsdirektör (t.o.m. den 31 december 1983)

Sekreterare:
Ledell, Göran, avdelningsdirektör (t.o.m. den 30 september 1983)
Osvald, Thomas, byråchef (fr.o.m. den 1 juni 1984)
Pålsson, Ulla, hovrättsfiskal (t.o.m. den 31 oktober 1983)

Bitr. sekreterare:
Thulstrup, Jörgen, departementssekreterare (fr.o.m. den 1 november 1984 t.o.m. den 15 oktober 1985)

Statens offentliga utredningar 1986

Kronologisk förteckning

1. Översyn av rättegångsbalken 2. Högsta domstolen och rättsbildningen. Ju.
2. En treårig yrkesutbildning – riktlinjer. U.
3. En treårig yrkesutbildning – beskrivningar, förslag. U.
4. Bostadskommitténs slutbetänkande. Sammanfattning. Bo.
5. Bostadskommitténs slutbetänkande. Del 1. Bo.
6. Bostadskommitténs slutbetänkande. Del 2. Bo.
7. Militära skyddsområden. Fö.
8. Soliditet och skälighet i försäkringsverksamheten. Fi.
9. Ny lönegarantilag. A.
10. Enklare skolförfattningar. Del 1. Sammanfattning, kommittéförslag. U.
11. Enklare skolförfattningar. Del 2. Motiv m. m. U.
12. Datorer, sårbarhet, säkerhet. Fö.

Statens offentliga utredningar 1986

Systematisk förteckning

Justitiedepartementet

Översyn av rättegångsbalken 2. Högsta domstolen och rättsbildningen. [1]

Försvarsdepartementet

Militära skyddsområden. [7]
Datorer, sårbarhet, säkerhet. [12]

Finasdepartementet

Soliditet och skälighet i försäkringsverksamheten. [8]

Utbildningsdepartementet

En treårig yrkesutbildning – riktlinjer. [2]
En treårig yrkesutbildning – beskrivningar, förslag. [3]
Enklare skolförfattningar. Del 1. Sammanfattning, kommittéförslag. [10]
Enklare skolförfattningar. Del 2. Motiv m. m. [11]

Arbetsmarknadsdepartementet

Ny lönegarantilag. [9]

Bostadsdepartementet

Bostadskommitténs slutbetänkande. Sammanfattning. [4]
Bostadskommitténs slutbetänkande. Del 1. [5]
Bostadskommitténs slutbetänkande. Del 2. [6]

KUNGL. BIBL.
1986-04-02
STOCKHOLM

Anm. Siffrorna inom klammer betecknar utredningarnas nummer i den kronologiska förteckningen.

Liber
Allmänna Förlaget

ISBN 91-38-09198-4
ISSN 0375-250X