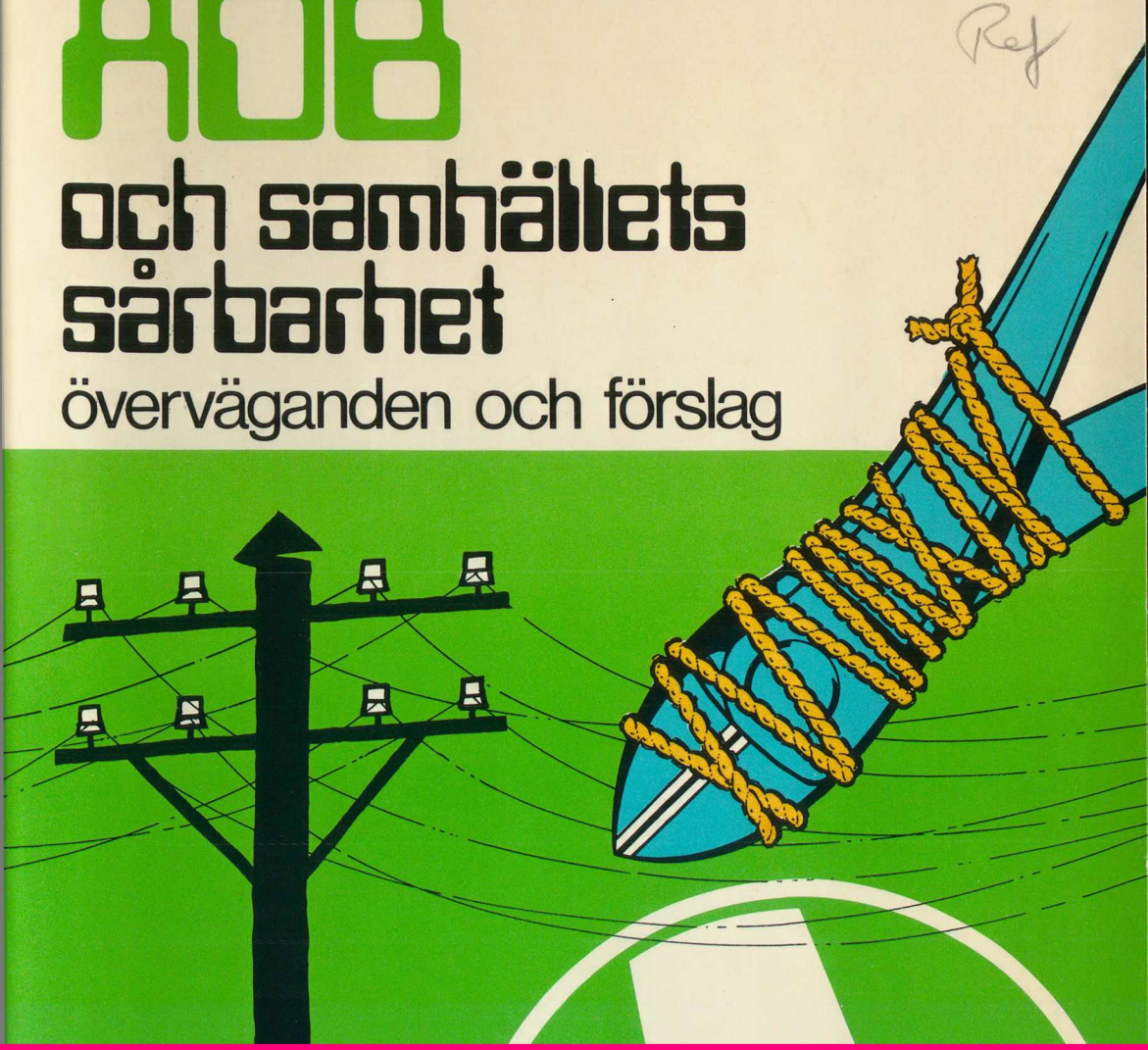
ROB

och samhällets sårbarhet

överväganden och förslag



SOU
979:93

Betänkande av sårbarhets-kommittén (SÅRK)

ADB och samhällets sårbarhet

överväganden och förslag

SOU 979:93

Betänkande av sårbarhets-kommittén (SÅRK)

Statens offentliga utredningar
1979:93
Försvarsdepartementet

ADB och samhällets sårbarhet

Överväganden och förslag

Betänkande av sårbarhetskommittén (SÅRK)
Stockholm 1979

Omslag Bertil Ankarberg
Jernström Offsettryck AB

ISBN 91-38-05328-4
ISSN 0375-250X
LiberTryck, Stockholm 1979

Till Statsrådet och chefen för försvarsdepartementet

Genom beslut den 28 april 1977 bemyndigade regeringen chefen för försvarsdepartementet att tillkalla en kommitté med högst åtta ledamöter för att utreda frågan om datasystemens sårbarhet och föreslå åtgärder i syfte att minska denna. Med stöd av detta bemyndigande förordnade departementschefen den 26 maj 1977 som ledamöter kanslirådet Allan Eriksson, tillika ordförande, överdirektören Ulf Carlsson, generaldirektören Jan Freese, avdelningsdirektören Olof Hertz, civilingenjören Johan Martin-Löf, avdelningsdirektören Ulf Tengelin och direktören Per-Gunnar Vinge.

Samma dag förordnades till huvudsekreterare byråchefen Hans Wranghult och till sekreterare kammarrättsassessorn Bengt Siversen.

Att som expert biträda utredningen förordnades den 16 januari 1978 kammarrättsassessorn Ulrika Tengelin.

Kommittén har antagit namnet sårbarhetskommittén (SÅRK).

Den 21 juni 1978 har SÅRK till statsrådet överlämnat en lägesrapport, kallad ADB och samhällets sårbarhet (Ds Fö 1978:4). Lägesrapporten redovisar en första kartläggning av sårbarhetsproblematiken och en kort summering av SÅRKs slutsatser. Vidare innehåller lägesrapporten förslag till vissa riktlinjer för det fortsatta arbetet.

SÅRK får härmed överlämna sitt slutbetänkande. Detta innehåller en kompletterande kartläggning som huvudsakligen bygger på vad som framkommit vid remissbehandling av lägesrapporten. I slutbetänkandet framläggs även förslag till åtgärder för att minska samhällets sårbarhet till följd av ADB-användning.

Uppdraget är därmed slutfört.

Reservation har avgivits av ledamöterna Hertz och Vinge.

Särskilt yttrande har avgivits av ledamoten Freese.

Stockholm den 5 december 1979.

Allan Eriksson

Ulf Carlsson *Jan Freese* *Olof Hertz*

Johan Martin-Löf *Ulf Tengelin* *P-G Vinge*

/Hans Wranghult,
Bengt Siversen

Innehållsförteckning

Förkortningslista

ADB	Automatisk databehandling
ALLFA	Utredningen om ADB inom den allmänna försäkringen m m
AMS	Arbetsmarknadsstyrelsen
ARKSY	Arkivstatistiskt system
CBR	Centrala bilregistret
CFD	Centralnämnden för fastighetsdata
CFR	Centrala företagsregistret
CKR	Centrala körkortsregistret
COM	Computer Output Microfilm
CSN	Centrala studiestödsnämnden
CSTP	Committee for Scientific and Technological Policy
DAFA	Datamaskincentralen för administrativ databehandling
DALK	Datalagstiftningskommittén
DASK	Datasamordningskommittén
DI	Datainspektionen
EMP	Electromagnetic pulse
FOA	Försvarets forskningsanstalt
FRI	Försvarets rationaliseringsinstitut
ICCP	Working Party on Information, Computer and Communication Policy
IPF	Information i prognosfrågor
JK	Justitiekanslern
KF	Kooperativa förbundet
K-PAI	Kommunernas personaladministrativa informationssystem
LMV	Statens lantmäteriverk
LO	Landsorganisationen
LON	Länsstyrelsernas organisationsnämnd
MI	Miljövårdens informationssystem
MIS	Management Information System
NIMS	Nordiskt informationssystem och metoder för samhällsplanering
NPDN	Nordiskt allmänt datanät
PAR	Postens adressregister
PKN	Produktkontrollnämnden
REX	Riksdatasystemet inom exekutionsväsendet

RFV	Riksförsäkringsverket
RPS	Rikspolisstyrelsen
RRV	Riksrevisionsverket
RSDB	Regionalstatistisk databas
RSV	Riksskatteverket
RTB	Registret över totalbefolkningen
SAF	Svenska arbetsgivareföreningen
SCB	Statistiska centralbyrån
SFS	Svensk författningssamling
SIND	Statens industriverk
SIPU	Statens institut för personaladministration och personalutbildning
SIS	Standardiseringskommissionen i Sverige
SITA	Société Internationale de Telecommunications Aeronautiques
SJ	Statens järnvägar
SLÖR	Statligt löneuträkningssystem
SOU	Statens offentliga utredningar
SPADAB	Sparbankernas Datacentraler AB
SPAR	Samordnat person- och adressuppdateringsregister
SPK	Statens pris- och kartellnämnd
SPP	Svenska Personal-Pensionskassan
SSLP	Sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret
STU	Styrelsen för teknisk utveckling
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SÖ	Skolöverstyrelsen
TCO	Tjänstemännens centralorganisation
TSV	Trafiksäkerhetsverket
UHÄ	Universitets- och högskoleämbetet
UC	Upplysningscentralen
VPC	Värdepapperscentralen
VPV	Värnpliktsverket
ÖB	Överbefälhavaren
ÖEF	Överstyrelsen för ekonomiskt försvar

Sammanfattning

1 Inledning

Enligt beslut av regeringen tillsatte försvarsministern 26 maj 1977 sårbarhetskommittén (SÅRK) med uppgift att utreda sårbarheten hos det datoriserade samhället och att föreslå åtgärder för att minska denna.

Utredningsuppdraget

Utredningsuppdraget är inte begränsat till att motverka risker i samband med beredskap och krig utan tar även sikte på andra hot- och påtryckningssituationer. Som en särskild faktor nämns i direktiven den växande terrorismen i världen. SÅRK delar upp sårbarhetsfaktorerna i två huvudkategorier, yttre och inre. Den första tar sikte på olika angrepp utifrån t ex krigshandlingar och terroristaktioner. Den andra omfattar sådana faktorer som ligger mer eller mindre inbyggda i själva datorutnyttjandet, t ex datordriftens koncentration, beroendet av kompetent personal och bistånd från utlandet. SÅRK skall arbeta utifrån ett totalförsvarsperspektiv. Mot denna bakgrund konstaterar SÅRK att de angrepp och skador som skall ägnas intresse bör vara av relativt omfattande och ingripande karaktär för samhället i stort. SÅRKs arbete är inte begränsat till persondatafrågor. Även dataflödet av andra data skall kartläggas. Uppdraget omfattar även att göra en framtidsbedömning.

Redovisning av uppdraget

Vad gäller redovisningen av uppdraget har SÅRK valt att göra denna etappvis. I juni 1978 presenterade SÅRK en lägesrapport som omfattar en första kartläggning och en kort summering av SÅRKs slutsatser. Rapporten har remissbehandlats. Remissvaren har beaktats i slutbetänkandet.

I syfte att kartlägga vissa större datoranvändares bedömningar i sårbarhetsfrågor intervjuade SÅRK våren 1978 ett antal större användare. Vidare har SÅRK intervjuat några leverantörer av datorutrustning i syfte att få synpunkter på utlandsberoendet.

I slutbetänkandet återges vissa delar av lägesrapporten. Detta gäller

avsnitten om de olika sårbarhetsfaktorerna. De nyskrivna delarna består i huvudsak av visst fortsatt kartläggningsarbete samt av överväganden och förslag till åtgärder.

2 Sårbarhetsfaktorer

I beskrivningen av olika sårbarhetsfaktorer behandlas först yttre och sedan inre faktorer.

Kriminella handlingar

De kriminella handlingar som bör ägnas uppmärksamhet skall vara av relativt allvarlig art samt ha sådan inriktning att de allvarligt stör samhället. De brottsliga angrepp som är av störst intresse är av typen sabotage, spionerі etc. Även andra typer av brott kan ha intresse, t ex olika förmögenhetsbrott. Den ökade datoriseringen av betalningstransaktioner kan ge upphov till förmögenhetsbrott av helt nya dimensioner. SÅRK ägnar särskild uppmärksamhet åt terrorism och pekar bl a på att vissa författare hävdat, att terrorism med politisk inriktning i framtiden kan bli ett medel för aggression mellan stater vid sidan av konventionella krig. Vidare lämnas korta redogörelser för inträffade databrott i Sverige och utomlands. Bl a beskrivs olika terroristangrepp mot datacentraler i Italien, något som för övrigt föranlett särskild strafflagstiftning i detta land.

SÅRK konstaterar att det i dag förekommer databrottslighet av olika slag, att sådan brottslighet ofta är oerhört svår att upptäcka och att de brott som hittills uppdagats säkerligen endast utgör en bråkdel av dem som begåtts. Stora datamängder, möjligheten att bearbeta dessa data, datakommunikation etc kommer att ge ökade risker för olika former av spionerі. Eftersom datorer och datasystem redan utgjort mål för terroristverksamhet utomlands finns skäl att tro att sådan verksamhet även kan komma att rikta sig mot datacentraler i Sverige.

Missbruk för politiska syften

SÅRK gör bedömningen att hot om ekonomiska sanktioner — och ytterst förverkligande av sådana hot — framdeles kan bli ett allt vanligare påtryckningsmedel att nå politiska mål. Med tanke på att vi i hög grad är beroende av import inom datorområdet både vad gäller material och tjänster kan denna sektor bli ett attraktivt objekt för angrepp — låt vara ett av flera — vid olika former av ekonomisk krigföring. Redan en begränsad blockad mot import av reservdelar skulle mycket snabbt kunna få betydande effekter.

Genom att Sverige är beroende av internationella dataöverföringar och ledningar som passerar flera länder är vi även beroende av den

politiska situationen i andra länder. Databehandling utomlands ökar förutsättningarna för illasinnade grupper eller länder att utöva påtryckningar genom hot om avstängning av ledningar eller andra hinder för svenska kunder att utnyttja utländska datorer. Beroendet av utländsk personal för felsökning och reparation är även stort.

Inför en förestående väpnad konflikt får man även räkna med att aktiviteter som spionerі och liknande brott får en ökad intensitet. Infiltration bland personer med centrala uppgifter inom viktiga datasystem kan vara ett sätt att underlätta sabotage, spionerі och möjligheten att skapa förvirring bland allmänheten.

Krigshandlingar

Försvarsmaktens datorutnyttjande är inriktad mot en systemstruktur för både krig och fred. Vad gäller civila statliga myndigheters informationsbehandling i krig har regeringen givit särskilda föreskrifter. Dessa går i korthet ut på att sådana myndigheter i krigstid får räkna med en betydligt mindre ADB-användning än i fredstid. Även inom den kommunala och privata sektorn måste man räkna med att ADB-verksamheten måste krympas i krigstid.

Vid ett angrepp med konventionella vapen mot Sverige kan vissa delar av eller hela landet komma att besättas av fientliga styrkor. På grund av koncentrationen av datorkraft till storstadsområden kan ockupation av relativt begränsade delar av landet medföra att stora delar av landets ADB-system sätts ur spel. Koncentrationen medför även ökad sårbarhet vid bombangrepp och sabotage.

Inför en hotande ockupation kan det finnas skäl att undanföra eller förstöra datoranläggningar och olika register för att hindra att anläggningarna eller viktig information kommer i fientlig hand. Fienden kan t ex ha intresse av att komma över befolkningsregister och andra register som kan underlätta krigföringen. I särskild lag med följdförfattningar regleras frågor om undanförsel och förstöring. Någon specialreglering beträffande datorer och dataregister finns inte. Det kan finnas skäl att fortlöpande se över planeringen beträffande vilka datasystem som skall förstöras eller undanskaffas vid en krigssituation.

En annan faktor som påverkar sårbarheten vid ett krig är det ökade beroendet mellan olika datasystem som bl a innebär att utslagningen av ett system kan få återverkningar på flera andra.

Ytterligare en viktig faktor är personalsidan. En stor del av den personal som behövs för den civila datordriften i krigstid måste vid ett krig användas inom det militära försvaret.

Vad gäller reservdelsförsörjning, service från utlandet etc uppstår avsevärda svårigheter vid ett krig.

Om kärnvapen kommer till användning måste man även räkna med den s k EMP (electromagnetic pulse)- effekten som kan slå ut eller störa datorer och kommunikationssystem. Särskilt höghöjdsexplosioner kan ge verkningar med stor utbredning — det kan röra sig om flera hundra mil. Skydd mot EMP-effekten är dyrt att anskaffa.

Katastrofer och olyckshändelser

Vad gäller yttre händelser tas slutligen katastrofer och olyckshändelser upp. Det är alltså fråga om oavsiktliga yttre händelser. Hit hör naturkatastrofer av olika slag. Katastrofer kan även uppstå genom att farligt gods exploderar, genom överslag i elkablar genom brand etc. Sverige har varit relativt förskonat från stora naturkatastrofer.

Katastrofer och olyckor kan både direkt och indirekt påverka verksamheten vid ADB-drift. Dels kan själva anläggningen skadas eller förstöras, dels kan driften störas genom avbrott i el- och vattenförsörjningen. Längre strömavbrott i storstadsområden skulle i dag kunna få besvärande följder för många ADB-användare.

Ras eller liknande katastrofer händer relativt sällan. Att ett sådant ras skulle inträffa på platsen för en datoranläggning ter sig som något relativt osannolikt. Placering av viktiga datoranläggningar i riskområden som t ex områden med rasrisk eller nära storflygplatser bör dock undvikas.

Innehållsmässigt känsliga register

Bland de inre sårbarhetsfaktorerna diskuteras först innehållsmässigt känsliga register av olika slag.

Vad gäller befolkningsregistren konstaterar SÅRK att i datalagen (1973:289) har införts en 3 a § som kan bidra till att minska spridningen av befolkningsregister men att en del befolkningsregister likväl kommer att finnas kvar. En översiktlig beskrivning görs av några av de mest omfattande befolkningsregistren, bl a riksförsäkringsverkets register, folkbokförings- och skatteregistren samt bil- och körkortsregistren. Särskilt nämns koordinatsatta personband hos centralnämnden för fastighetsdata. SÅRK pekar på vissa risker som kan vara förknippade med befolkningsregister. Vid olika krigs- och krissituationer kan sådana register vara ett hjälpmedel för en angripare att nå kontroll över befolkningen och att plocka fram nyckelpersoner av olika slag. Detta gäller framförallt om ett flertal register kan sambearbetas. Ett särskilt utmärkt hjälpmedel i detta sammanhang är de koordinatsatta personbanden utbyggda med annan personinformation. Exempelvis skulle olika grupper av särskilt intresse kunna plockas ut och placeras geografiskt på olika sorters kartor genom s k karteringar. Eftersom koordinaterna är knutna till fastighet sker lägesbestämningen med relativt god precision. Uppgifter om persondata kompletterad med information om bostads- och uppehållsort ger en ockupationsmakt stora möjligheter till kontroll av befolkningen inom det ockuperade området. Är uppgifterna dessutom åtkomliga från terminal i rörliga enheter torde kontrollen av befolkningens rörelser kunna bli mycket effektiv.

SÅRK pekar vidare på att vissa register kan innehålla så känslig personinformation att de kan ha intresse från sårbarhetssynpunkt. Sådan registerinformation kan i orätta händer användas för obehöriga påtryckningar av olika slag.

En annan typ av innehållsmässigt känsliga register är sådana som innehåller företagsuppgifter och liknande information. Bl a påpekas att ett stort antal myndigheter har rätt att inhämta i princip alla de uppgifter de anser sig behöva för sin verksamhet. Under senare år har därför allt större mängder företagsdata lagrats i offentliga datasystem. Annan information som nämns här är bl a uppgifter om vägnätet (vägar, broar etc), som finns lagrad i vägverkets databank. Vidare nämns att i vissa kommunala ADB-system kan finnas tekniska och geografiska detaljbeskrivningar t ex rörande el, vatten, avlopp och gas.

Funktionellt känsliga system

Ett stort antal känsliga samhällsfunktioner är datoriserade. Som exempel kan nämnas bl a riksförsäkringsverkets olika register, som används för att administrera ett omfattande ekonomiskt trygghetssystem, bankverksamheten där betalningströmmarna alltmer har datoriserats, varuhandeln med datorstödd distribution, lagerhållning etc. Vidare kan nämnas system för processtyrning där datorerna används för övervakning och styrning av produktionsprocessen inom järn- och stålverk, pappersbruk etc, system för produktionsstyrning inom tillverkningsindustrin, system för trafikstyrning etc. Störningar i system av nu nämnt slag kan snabbt ge effekter i form av försenade eller uteblivna betalningar, svårigheter att få ut order till verkstäderna med produktionsstörningar till följd, bristande kontroll över lager och distribution med åtföljande varubrist och produktionsstörningar, störningar i trafiken m m.

Koncentration

SÅRK skiljer på geografisk och funktionell koncentration av ADB-driften. Med geografisk koncentration menas stor ansamling av datorkraft till vissa områden. Med funktionell koncentration avses stora centrala system eller stora servicebyråer med central drift och många kunder. SÅRK konstaterar att både geografisk och funktionell koncentration förekommer i betydande omfattning och finner att en ökad -- funktionell och geografisk — spridning av datorkraften kan ha betydande fördelar från sårbarhetssynpunkt. Som skäl nämns bl a att utslagningen av en mindre enhet aldrig kan få lika förödande följder som utslagningen av ett stort centralt system. Vad gäller den geografiska spridningen ger den fördelar framförallt i en krigs- eller beredskapssituation.

Integration och inbördes beroende

Ett omfattande informationsflöde förekommer i dag mellan olika datasystem. Även informationsutbyte genom dator till datorförbindelse sker i dag och kommer att bli allt vanligare. Olika system är beroende av att få information från andra. Även ett systemberoende har uppkommit

genom att olika system för att kunna kommunicera med varandra måste tillämpa samma procedurer och standarder i en rad avseenden. Redan i dag förekommer alltså ett avsevärt beroende och den framtida utvecklingen främst på kommunikationssidan kan komma att öka detta beroende. Från sårbarhetssynpunkt innebär detta att skador, störningar eller felaktigheter i ett system får negativa återverkningar i en rad andra.

Bearbetningsmöjligheter vid ansamling av stora datamängder

Användningen av ADB gör det möjligt att sammanföra och överblicka mycket stora kvantiteter information. Stora datamängder finns t ex hos statistiska centralbyrån men även på många andra ställen inom den offentliga och privata sektorn. Det rör sig inte bara om personuppgifter utan även om uppgifter om företag, fastigheter, vägar och broar, olika produkter etc.

Sedan gammalt har underrättelseverksamhet bedrivits genom sammanställning av ett stort antal i och för sig banala och ofta offentliga uppgifter varigenom slutsatser kunnat dras i frågor som är omgivna av militär och kommersiell sekretess. Användningen av ADB ger här helt nya möjligheter. I Sverige används datorer i viss utsträckning vid försvarsstabens underrättelseavdelning. Att datorer används av andra länders underrättelsetjänst kan man utgå ifrån. Vid planläggning av och vid ett eventuellt genomförande av angrepp mot vårt land kan en främmande makt ha stor nytta av ADB-lagrade uppgifter om geografiska förhållanden (vägar, järnvägar, broar m m), om vår produktionsapparat (kapacitet och lokalisering) och om vår kraftförsörjning m m.

Bristfällig utbildning

De flesta av de myndigheter och företag som SÅRK intervjuat uppfattade inte bristfällig utbildning och kunskap hos datoranvändare som någon påtaglig sårbarhetsfaktor. SÅRK konstaterar dock att man inte kan bortse från betydelsen av utbildning när sårbarhetsfrågor diskuteras och förordar en förstärkt utbildning på olika nivåer där vikt även läggs vid säkerhets- och sårbarhetsfrågor.

Bristande kvalitet i fråga om maskin- och programvara

Bristande kvalitet i fråga om maskin- och programvara förefaller SÅRK, bl a på grund av vad som framkommit vid intervjuarbetet, inte vara någon allvarlig sårbarhetsfaktor. I många fall måste man dock ställa mycket stora krav på att systemen fungerar t ex vid trafikstyrning där fel kan leda till allvarliga olyckshändelser. Vidare kan fel i programvara som inte upptäcks på en gång ge skador som senare är omöjliga att reparera. I viktiga och känsliga system kan sådana skador få allvarliga konsekvenser.

Nyckelpersoner för datordriften

SÅRK konstaterar att systemerare och programmerare kan bygga upp komplicerade system som ingen annan än de själva behärskar. Saknas dokumentation eller är dokumentationen bristfällig kommer användaren i händerna på systembyggaren.

Flera exempel finns även på att missnöjda, ohederliga eller opålitliga medarbetare åsamkat skador t ex genom att förstöra registerinformation.

SÅRK berör sedan behovet av personalkontroll. Endast vad gäller den statliga sidan finns författningsreglerad sådan och den rör i vissa fall även ADB-personal. SÅRK konstaterar att personalkontroll inte är något fullständigt effektivt instrument.

Vid beredskap och krig får beroendet av ADB-personal särskild betydelse. En stor del av denna personal utgörs av värnpliktiga i befäls- och specialistfunktioner, något som gör att de militära myndigheterna inte vill avvara dem. Inför en krigssituation kan ADB-personal även tänkas utgöra en grupp nyckelpersoner i samhället som en fiende skulle kunna tänkas vilja oskadliggöra.

Även vid konflikter på arbetsmarknaden kan beroendet av ADB-personal utnyttjas. Stora effekter kan åstadkommas genom att enbart sådan personal tas ut i strejk.

Dokumentation

Det förekommer ofta att fortlöpande förändringar i ADB-system av tidsskäl och ekonomiska orsaker inte dokumenteras på ett tillfredsställande sätt. Behovet av dokumentation gör sig särskilt gällande i samband med övergång från en generation datorer till en ny eller vid byte till annat fabrikat, liksom vid driftstörningar eller personalomsättning. När användaren anlitar utomstående datorkraft och det är fråga om unika system är risken stor att användaren blir strandsatt om servicebyrån av någon anledning inte fungerar. I en sådan situation saknar användaren vanligen tillräcklig dokumentation.

Vid SÅRKs intervjuarbete framkom att många användare ansåg sig ha fullgod dokumentation medan andra menade att den var bristfällig och att detta innebar sårbarhet.

Katastrofberedskap

Det mest väsentliga för en katastrofberedskap är att en planering för katastrofsituationer föreligger. Beredskapen skall dessutom omfatta kontroll av att utarbetade planer fungerar. Syftet med katastrofplanering är att om allvarlig skada inträffar så skall konsekvenserna av sådan skada motverkas och mildras så mycket som möjligt. Brister i katastrofplaneringen kan få förödande följder, åtminstone om skador inträffar i för samhället viktiga datasystem. SÅRKs intervjuundersökning har visat att katastrofberedskapen på många håll inte är vad den borde vara.

Utlandsberoende

SÅRK finner att behovet av komponenter, reservdelar och service från utlandet m m gör vårt land beroende av att det internationella handelsutbytet flyter utan allvarligare störningar. Man kan utgå från att vår reservdelslagring, våra möjligheter till egen tillverkning och våra möjligheter till inhemsk service skulle möjliggöra datordrift i nuvarande omfattning endast under kortare tid om störningar skulle uppstå på grund av krig, avspärrningar, handelsblockader o dyl. Det finns skäl att anta att det beroende som nu diskuteras kommer att öka.

Det ökade dataflödet över gränserna medför säkerhets-och sårbarhetsproblem av andra dimensioner än de som finns om man ser endast på rent nationella förhållanden. Om databehandlingen sker på en dator som finns i ett annat land eller på en annan kontinent, och om in- och utdata skall passera genom flera länder ökar därmed även riskerna för angrepp av olika slag. Att skydda sig mot händelser utom riket är av naturliga skäl svårare än att bygga upp ett inhemskt skydd.

3 Fortsatt kartläggning

Den fortsatta kartläggningen har inte lett till några omfattande kompletteringar. Det som redovisas i kapitel 6 bygger delvis på synpunkter och material som kommit fram i remissvaren.

Datakommunikationsteknik

Frågor som gäller datakommunikationer behandlas något utförligare bl a det allmänna datanätet och kommunikationer över satellit. SÅRK pekar även på en del allmängiltiga frågor. Det sägs bl a att det inte är helt ovanligt att system görs onödigt komplicerade genom att krav ställs på snabba informationsflöden inom eller mellan olika system utan att behovet därav är särskilt starkt. Många gånger kan informationen med bibehållen servicegrad hämtas på enklare sätt och således utan avancerade datakommunikationslösningar.

Innehållsmässigt känsliga register och funktionellt känsliga användningsområden

Genom remissvaren har en del ytterligare material av intresse kommit fram. Lantmäteriverket pekar på att olika typer av landskapsinformation kan ha ett värde för den som driver underrättelseverksamhet. Sålunda sägs att triangelpunkter, tyngdkraftsdata och höjddata kan utnyttjas för ledning av indirekt eld. På senare tid märks särskilt utvecklingen av kryssningsrobotar, vilka kan styras bl a med stöd av i robotarna datalagrad landskapsinformation. Enligt lantmäteriverket är det mycket svårt att skydda hemliga uppgifter inom bl a området för landskapsinformationen i och med att informationen kan hanteras med ADB.

Utöver de funktionellt känsliga områden som tidigare berörts bör även nämnas den grafiska industrin, som blivit alltmer datoriserad.

I samband med de innehållsmässigt känsliga registren diskuteras även användningen av kryptering och behörighetssystem. SÅRK framhåller att användning av kryptering och behörighetssystem — liksom andra säkerhetsåtgärder — givetvis kan bidra till att minska den sårbarhet som sammanhänger med känsliga register även om dessa hjälpmedel ingalunda ger ett komplett skydd. En ökad användning av kryptering får därför anses som angelägen. Genom att krypteringsmetoderna undan för undan förbättras underlättas även sådan användning. Förbindelsekryptering (kryptering av information som skall överföras genom datakommunikation) torde vara den som idag är den mest praktiskt användbara. Registerkryptering är dock i flertalet fall av större värde än förbindelsekryptering men är å andra sidan svårare att hantera.

Vad gäller behörighetssystem kan en del leverantörer idag erbjuda olika färdiga anordningar inbyggda i maskin- och programvaran.

Möjligheten att sprida datorkraft

Den tekniska utvecklingen fortsätter i sådan riktning att en spridning av datorkraften underlättas.

Framförallt blir datorerna allt mindre, snabbare och billigare. Detta innebär att pris och teknik medger att varje användare, det gäller myndighet eller annan, kan skaffa sig datorer och system som passar just honom. Denna utveckling medför positiva effekter från sårbarhetssynpunkt men kan även bli orsak till nya sårbarhetsproblem.

Utlandsberoende

Utlandsberoende finns även vad gäller programvara och behörighetssystem.

SÅRK har, av en del remissinstanser, fått stöd för sin uppfattning att det i vissa fall kan finnas skäl att granska bearbetningar som sker utomlands.

Standardisering

Standardisering av maskin- och programvara, dokumentation m m kan, enligt SÅRKs mening, bidra till minskad sårbarhet bl a genom att ge bättre back-up-möjligheter, minskat personalberoende och även minskat utlandsberoende. Det är därför väsentligt att ett fortlöpande arbete sker inom detta område och att standardiseringsfrågor även beaktas i samband med upphandling.

Ansvaret för ADB-frågor m m inom regeringskansliet och hos olika myndigheter.

I kapitel 7 redogör SÅRK för vissa departements och myndigheters ansvar för ADB, totalförsvar m m. Kapitlet ger bl a underlag för över-

väganden om vilken myndighet som bör åläggas huvudansvaret för sårbarhetsfrågor. Bland de myndigheter som beskrivs kan nämnas datainspektionen, överbefälhavaren, televerket, statskontoret och överstyrelsen för ekonomiskt försvar.

Pågående datapolitisk utveckling

Kapitel 8 behandlar den pågående datapolitiska utvecklingen i de delar som berör sårbarhetsproblemen. Huvudpunkterna i propositionen, 1978/79:121, Användning av ADB i statsförvaltningen beskrivs. I propositionen föreslås bl a att formella regler utfärdas för etappindelning, beslutspunkter och beslutsunderlag i samband med systeminvesteringar. Reglerna för beslut om större och viktigare investeringar samlas i en särskild handläggningsordning. För datordriften anges två huvudprinciper. Den ena är att datordrift som är av större omfattning skall ske för varje verksamhet för sig. Den andra är att datordriften inom en verksamhet på lämpligt sätt bör spridas bl a med tanke på sårbarheten. Riksdagen godtog huvudprinciperna i propositionen. Riksdagen beslutade även att inrätta en datadelegation knuten till regeringskansliet. Delegationen skall bl a tillgodose parlamentarisk bevakning av sårbarhets- och säkerhetsfrågor.

I kapitlet redogörs även för olika statliga utredningar inom ADB-området, bl a några med näringspolitisk inriktning. Där finns slutligen avsnitt som rör internationellt samarbete och internationella datanät.

Behandling av sårbarhetsfrågor i vissa främmande länder.

Såvitt SÅRK har kunnat finna har inte några övergripande offentliga utredningar gjorts utomlands om det datoriserade samhällets sårbarhet. Ett ökande intresse kan dock skönjas för dessa frågor även i andra länder. Många av de delfrågor SÅRK arbetar med har för övrigt diskuterats ingående utomlands t ex olika slags brottslighet riktat mot ADB-verksamhet och beroendet av ADB-verksamhet utanför det egna landets gränser. I utländsk datalagstiftning kan man även finna exempel på bestämmelser som enligt svenskt synsätt rör sårbarhetsaspekter.

4 SÅRKs överväganden

SÅRK har utgått från att det tekniskt utvecklade samhället inte kan undvara ADB-tekniken. Samtidigt har SÅRK pekat på en mängd risker som hör samman med användningen av ADB. Den redovisning som gjorts kan ge ett intryck som leder till ett alltför pessimistiskt synsätt. Kartläggningen leder emellertid fram till den allmänna slutsatsen att sårbarheten är oacceptabelt hög i dagens genomdatoriserade samhälle. Den fortgående utvecklingen leder till en allt högre sårbarhet om inte motåtgärder vidtas. Olika händelser och angrepp kan ge omfattande störningar och skador även vid djupaste fred. ADB-användning är endast en av flera orsaker till det moderna samhällets sårbarhet. Detta får

emellertid inte ursäkta att man underlåter att begränsa den sårbarhet som är betingad av ADB-användning så länge en sådan begränsning kan uppnås med rimliga medel.

Sårbarhet beroende på ADB-användning

När det gäller ADB föreligger ett betydande importbehov och därav följande sårbarhet. Till detta kommer ett inte obetydligt importberoende av datatjänster i form av bearbetningar utomlands. Vid sidan av utlandsberoendet står ett flertal sårbarhetsfaktorer att finna inom landet. Beredskapen mot kriminella handlingar, missbruk för politiska syften och krigshandlingar är många gånger obefintlig eller i varje fall otillräcklig. Datoriseringen har medfört funktionellt känsliga system. Vidare har ADB-driften koncentrerats både funktionellt och geografiskt på ett sätt som knappast vittnar om att sårbarhetsfaktorer beaktats. De risker koncentrationen vållar kan förstärkas genom en långt driven integration mellan framförallt de centrala systemen. I de centrala systemen ingår även vanligtvis innehållsmässigt känsliga register. Enligt SÅRKs uppfattning föreligger sårbarhet främst beträffande de stora centrala systemen och datoranläggningarna.

Orsaker till rådande förhållanden

Statsmakterna har inte styrt den utveckling som lett fram till dagens genomdatoriserade samhälle. Någon övergripande bedömning har inte gjorts av de risker som den sammantagna datoriseringen av olika samhällsområden leder till.

Några riktlinjer har heller inte meddelats, förmodligen beroende på bristande medvetenhet och förutseende vad gäller sårbarhetsproblem förknippade med ADB-utvecklingen. De personella resurserna har dessutom ofta varit alltför knappa för att möjliggöra alla de bedömningar SÅRK nu finner påkallade. Trots att den fortsatta ADB-tekniska utvecklingen numera medger helt andra lösningar kommer det att ta mycket lång tid att förändra strukturen på dagens ADB-användning.

Åtgärder för att motverka sårbarheten

Enligt SÅRKs uppfattning kan sårbarheten begränsas i redan existerande system. Nya system bör genom en sårbarhetsbedömning kunna byggas upp annorlunda än hittills skett. Detta mål kan delvis nås genom information och rådgivning. Enligt SÅRKs mening är emellertid information och rådgivning inte tillräckligt verksamma medel beträffande sådan datoranvändning som är särskilt betydelsefull från sårbarhetssynpunkt. För sådan användning föreslår SÅRK längre gående åtgärder bl a krav på tillstånd. De tvingande åtgärder SÅRK föreslår förutsätter en lagreglering och det kan finnas skäl att samla de mera centrala reglerna i en särskild lag. SÅRK presenterar ett utkast till en sådan lag med arbetsnamnet sårbarhetslag (SÅRL). Däremot har SÅRK inte lagt

fram förslag till följdförfattningar. SÅRK har heller inte utarbetat detaljmotiv för de enskilda bestämmelserna i SÅRL. Sådana författningar och detaljmotiv bör enligt SÅRKs mening utarbetas först när statsmakterna tagit principiell ställning till SÅRKs förslag.

Ansvarig datoranvändare

Ansvaret för sårbarhetsfrågorna bör enligt SÅRKs mening primärt ligga på den som använder datorer som hjälpmedel i den egna verksamheten. Om han anlitar dataservicebyrå är möjligheterna att påverka sårbarheten i vissa avseenden beskurna. Ansvaret i dessa delar bör då i stället åvila servicebyrån. På den ansvarige ankommer det att göra tillståndsansökan m m och han blir även adressat för eventuella föreskrifter.

Tillståndsförfarande

Tillståndsprövningens innehåll.

SÅRK har pekat på en mängd olika sårbarhetsfaktorer. Samtliga faktorer får tas som utgångspunkt när ett system eller användningsområde granskas. De olika faktorerna kan emellertid slå olika hårt beroende på verksamheten. Åtgärder som minskar sårbarheten i något avseende kan öka den i ett annat. En sårbarhetsprövning måste därför göras från fall till fall och sårbarheten måste dessutom vägas mot andra faktorer som ekonomi, rationalitet etc.

En tillståndsprövning skall enligt SÅRK omfatta registerinnehåll, systemstruktur, ADB-säkerhet, personalberoende, maskinella och manuella reservrutiner, katastrofplanering, dokumentation, integration och beroende av andra databehandlingsystem, geografisk lokalisering samt lämpligheten av utlandsbearbetningar. I fråga om dessa punkter skall även erforderliga föreskrifter för att minska sårbarheten ges. Det kan då gälla vilket innehåll som får finnas i registren, vilka säkerhetsåtgärder som krävs, personalplanering, i vad mån utlandsbearbetningar får ske och vilka särskilda åtgärder som i så fall måste vidtas, vilka krav som bör ställas på dokumentation, katastrofplaner etc. I syfte att motverka koncentration bör möjligheterna att utnyttja distribuerad databehandling särskilt undersökas.

Endast i rena undantagsfall kan det bli aktuellt att vägra tillstånd till datordrift.

När ett register inte längre skall föras skall detta anmälas till den ansvariga myndigheten som skall föreskriva hur det skall förfaras med registren.

Tillståndsmyndigheten skall ha möjlighet att ge föreskrifter för sådan användning av dator som beslutats av statsmakterna om inte statsmakterna har gett föreskrifter i samma hänseende.

SÅRK har ansett att tillståndsplikten i princip skall gälla samtliga datoranvändningsområden. Den skall alltså omfatta olika administrativa tillämpningar med såväl personinformation som annan information

samt tillämpningar som gäller trafikstyrning, processtyrning etc. Tillståndsplikten går dock enligt förslaget olika långt inom den offentliga och den privata sektorn.

Tillståndsförfarandets omfattning inom den offentliga sektorn

SÅRKs förslag innebär att datoranvändning inom hela den offentliga sektorn med undantag av försvarsmakten skall underkastas en tillståndsprövning. Användning som uppenbarligen inte kommer att medföra risker från sårbarhetssynpunkt skall dock undantas genom en generell dispensregel. Vad som avses bli undantaget får bestämmas närmare av regeringen eller av myndighet som regeringen bestämmer enligt vissa allmänna riktlinjer.

Tillståndsplikten gäller inte sådan datoranvändning som beslutats av regering och riksdag. Före sådant beslut skall dock tillståndsmyndigheten höras.

Ett skäl för ett omfattande tillståndsförfarande inom den offentliga sektorn är att det inom denna finns många för samhället viktiga system. De är viktiga bl a därför att datorerna används för att administrera områden där betydelsefulla åtaganden finns från samhällets sida. Dessa områden kan vara mycket känsliga för störningar. Ett annat skäl är att i dessa system finns ofta bred, djup och känslig information. Ytterligare ett skäl är att många av de offentliga systemen är integrerade med varandra och även med system på den privata sektorn som därigenom många gånger är beroende och styrda av den offentliga ADB-verksamheten.

Inom försvarsmakten ingår bedömning av sårbarhetsfrågor som ett naturligt led i verksamheten för vilken det även finns ett övergripande ansvar hos överbefälhavaren. SÅRK har därför funnit det naturligt att låta försvarsmakten falla utanför lagens tillämpningsområde.

På den statliga sidan håller ökade möjligheter att styra ADB-användningen på att införas bl a genom den tidigare nämnda handläggningsordningen och genom att olika granskningsfunktioner inrättas. Enligt SÅRKs mening finns dock behovet en av myndighet som bedömer sårbarhetsfrågor kvar även vid en mer formaliserad handläggning av ADB-ärenden inom statsförvaltningen.

Tillståndsförfarandets omfattning inom den privata sektorn

För den privata sektorn föreslår SÅRK ett tillståndsförfarande beträffande ADB-baserade befolkningsregister och register över persongrupper som kan vara av intresse för underrättelsetjänst hos främmande makt.

De nämnda registren medför sådana risker från sårbarhetssynpunkt att tillståndsförfarande är nödvändigt. Beträffande frågan om tillstånd för övrig ADB-användning har SÅRK beaktat följande. Problem med datordriften drabbar ofta i första hand det enskilda företaget och inte samhället i stort. Vidare har man på den privata sidan ofta en helt annan ekonomisk press på sig vilket ibland medför större intresse för säkerhets-

och sårbarhetsfrågor än på den offentliga sektorn. SÅRK anser även att det i de flesta fall är möjligt att på frivillighetens väg, bl a genom råd och anvisningar, nå rimliga lösningar på olika sårbarhetsproblem inom denna sektor.

Tillsyn

Enligt förslaget skall det tillståndspliktiga området även stå under tillsyn. I samband med tillsynen kan ändrade föreskrifter ges och i undantagsfall kan meddelat tillstånd återkallas.

Anmälningsförfarande

För att underlätta rådgivningsverksamheten inom de viktigare delarna av den privata sektorn föreslår SÅRK ett anmälningsförfarande. Detta innebär en anmälningsplikt för datoranvändande företag och organisationer som anses som särskilt viktiga från sårbarhetssynpunkt. SÅRK har angett delar inom den privata sektorn som är särskilt betydelsefulla. Hit hör bl a bank- och försäkringsväsende, viss tillverkningsindustri, kommunikations- och transportväsende samt varuhandeln. För att få fram företag av intresse föreslår SÅRK att ÖEFs förteckning över s k K-företag skall användas. I denna förteckning finns de företag som ÖEF finner vara av särskild betydelse när det gäller att tillgodose landets behov av förnödenheter och tjänster under krig. Dessa företag torde i stort motsvara dem som är betydelsefulla i förevarande sammanhang. Det bör ankomma på regeringen att närmare ange vilka K-företag som skall omfattas av ett anmälningsförfarande.

Anmälan bör innehålla uppgifter om maskinell utrustning, dess lokalisering och användningsområde, systemstruktur, ADB-säkerhet, katastrofberedskap och typ av registerinnheåll. Anmälan skall alltid innehålla uppgift om vilka utlandsbearbetningar som förekommer.

En sådan anmälningsplikt underlättar en aktiv rådgivnings- och upplysningsverksamhet och ger dessutom nödvändigt underlag för den fortsatta diskussionen av frågor som rör sårbarhetssituationen i landet och hur denna skall bemästras.

Rådgivning och information

SÅRKs förslag innebär att endast vissa delar av samhällets datoranvändning skall omfattas av en tillståndsprövning. En utgångspunkt för SÅRK har emellertid varit att en aktiv rådgivnings- och informationsverksamhet skall förekomma inom såväl det tillståndspliktiga området som inom övriga områden. SÅRK anser att denna del av verksamheten måste ägnas stor uppmärksamhet. Rådgivnings- och informationsverksamheten kan ske genom uppsökande verksamhet, genom tryckta anvisningar och normer eller i andra lämpliga former.

Tillståndspliktiga användare skall även kunna begära bindande förhandsbesked av tillståndsmyndigheten.

Dataservicebyråverksamhet

Även dataservicebyråverksamhet skall omfattas av förslaget. Prövningen och föreskrifterna skall dock begränsas till de punkter för vilka ansvaret, helt eller delvis, naturligt ligger på servicebyrån. Främst gäller detta ADB-säkerhet, personalberoende, dokumentation, reservrutiner, katastrofplaner och utlandsbearbetningar. Servicebyråverksamhet inom den offentliga sektorn är enligt förslaget tillståndspliktig oavsett om verksamheten drivs av en myndighet eller av ett bolag som ägs av stat eller kommun.

Övergångsbestämmelser

SÅRKs förslag gäller i första hand nya tillämpningar och sådana som undergår väsentliga förändringar. För datoranvändning som påbörjats före ikraftträdandet gäller lagen när en övergångstid på fem år gått till ända om inte väsentliga ändringar gjorts dessförinnan, för vilket fall lagen gäller från tidpunkten för förändringen. Anmälan behöver, för användning som påbörjats före ikraftträdandet endast ske då väsentliga förändringar görs. Även för äldre tillämpningar förutsätts dock rådgivning kunna ske.

Myndighet för de föreslagna åtgärderna

I kapitel 17 diskuteras vilken myndighet som skall ges huvudansvaret för sårbarhetsfrågorna. Efter att ha inventerat vilka befintliga myndigheter som är tänkbara har SÅRK vägt främst mellan datainspektionen och överstyrelsen för ekonomiskt försvar. SÅRK har stannat för att föreslå datainspektionen. Datainspektionen skall alltså vara tillstånds-, tillsyns- och anmälningsmyndighet och får då även svara för rådgivning och information.

Talan mot datainspektionens beslut kan enligt förslaget föras hos regeringen. JK kan föra talan för att tillvarata allmänna intressen.

Rådgivande organ

SÅRK föreslår att ett rådgivande organ vad gäller sårbarhetsfrågor skall inrättas med representanter från berörda departement, myndigheter och näringslivsorganisationer. Det rådgivande organet skall knytas till datainspektionen och förutsätts i första hand ägna sig åt principiella övergripande frågor av intresse för olika sårbarhetsaspekter.

Överväganden kring andra åtgärder

I kapitel 18 tar SÅRK i korthet upp frågor som rör utlandsberoende och den svenska datorindustrins konkurrenskraft samt frågor som rör reservdelsförsörjning. Vidare diskuteras frågor som rör ansvaret för data-

kommunikationer, personalsamordning mellan militära och civila sidan, standardisering och utbildning samt skyddet för företag. Slutligen tas vissa problem upp, som sammanhänger med användning av annan teknik än datorteknik, bl a mikrofilms- och mikroficheteknik.

I Inledning

1 Utredningens direktiv

I direktiven för SÅRK anför chefen för försvarsdepartementet, statsrådet Krönmark, följande.

Utvecklingen på datateknikens område har varit synnerligen snabb. Nästan varje sektor inom samhället är idag beroende av en fungerande ADB-teknik. Datoriseringen har medfört att informationsbehandling och informationsflöde fått ett omfång som tidigare var otänkbart. Det kan med visst fog hävdas att vi lever i ett samhälle, där information har blivit en förutsättning för en effektiv administration.

Utvecklingen medför emellertid betydande risker. Det har blivit besvärligare att skydda informationen mot tillgrepp eller annat missbruk. Det har dessutom blivit väsentligt svårare att upptäcka att sådana handlingar har utförts. Spionage i olika former har underlättats medan motåtgärderna inte har utvecklats i samma takt. Stora delar av informationen har koncentrerats till ett begränsat antal databanker. Anmärkas kan att denna samlade information ofta kan vara åtråvärd även för andra syften än de för vilka informationen behörigen lagras och bearbetas. I vissa fall kan den lagrade informationen synas ointressant och risken för missbruk kan bedömas som liten. Men mängden lagrade data samt möjligheterna att med dator bearbeta dem för speciella syften skapar också möjligheter till missbruk.

Informationen som har lagrats i databanker kan ibland vara av så känslig natur att obehörig inte under några villkor bör få tillgång till den. Bearbetning av informationen kan leda till avslöjanden om levnadsförhållanden m m av så känslig natur att obehörig numera i väsentligt större omfattning än tidigare kan missbruka informationen för sina syften och till men för samhället. De stora befolkningsregistren kan också utnyttjas för politiska syften. Grupper inom och utom landet kan t ex förteckna kategorier av människor som har stor betydelse för landets administration eller försvar i syfte att sätta dem ur spel vid kriser eller krig.

Det finns befogad anledning att befara att datorer och datorlagrad information alltmer kan komma att användas för kriminella syften. I utlandet har händelser av sådan art redan inträffat. Så har t ex stulna datamedier utnyttjats för utpressning av ägareföretaget under hot om att dessa medier eljest skulle överlämnas till ett konkurrentföretag.

Inom varje samhällssektor ökar datasystemens inbördes beroende och de olika sektorerna blir, vad gäller informationsbehandling alltmer integrerade med varandra. Utredningen om företagens uppgiftsplikt har i sitt slutbetänkande (SOU 1976:12) visat att insamlingen av information till den statliga sektorn i mycket stor omfattning sker inom den privata sektorn. Ofta har informationsutbytet karaktären av massdataöverföring. Samhällets centrala databanker är idag beroende av att informationsutbytet mellan databehandlingssystemen och terminaltrafiken inte sviktar.

En kritisk faktor som i detta hänseende förtjänar uppmärksamhet är reservdelsförsörjningen i avspärrningslägen eller vid handelsbojkotter.

ADB-tekniken kan inte isoleras från annan teknik. Den kompletterar annan teknik och omvänt. Exempelvis har behovet och därmed beroendet av en fungerande telekommunikationsteknik och satellittrafik ökat. Inom en snar framtid ökar beroendet genom att ett svenskt allmänt datanät tas i drift som skall utgöra en del av ett gemensamt nordiskt nät. Detta kan längre fram väntas bli sammankopplat med andra nationella eller internationella datanät.

Flertalet datacentraler kan redan idag betraktas som utsatta mål såväl vid krig som vid hot och påtryckningar. De torde dessutom vara viktiga mål för grupper inom ett land som önskar störa samhällets funktioner. Inte minst servicebyråerna inom den privata sektorn är härvidlag av betydelse. En enda servicebyrå kan lagra och bearbeta information för 10 000-tals företag, som i sina skilda verksamheter är i hög grad beroende av att driften av deras datorsystem upprätthålls. Till bilden hör också att uppskattningsvis 80 % av all databehandling torde vara koncentrerad till storstadsområdena.

Datainspektionen har visat på det omfattande flödet av persondata över gränserna. Däremot saknas kunskap om hur vi är beroende av datorer i utlandet vad avser annan informationsbehandling. I den mån olika slag av data flödar över gränserna ökar beroendet av politiskt stabila förhållanden både i bearbetningslandet och i de länder genom vilka informationen transporteras.

Även beroendet av internationella databanker på skilda områden är otillfredsställande kartlagt.

Av stort intresse är i vad mån ADB-tekniken kan utnyttjas i krig. Inom försvarsmakten vidtas särskilda åtgärder för att säkerställa dess behov av datorkraft under beredskap och krig. För övriga delar av samhället utgår beredskapsplaneringen från antagandet att databehandlingen i samhället i sådana lägen kommer att bli mycket ringa. I de fall informationsbehandlingen bedöms kunna fortsätta har också kartlagts vilka datorer som överhuvudtaget kan användas på skilda orter. Situationen har emellertid förändrats såtillvida att en fortsatt databehandling på en ort sannolikt redan idag är på ett helt annat sätt än tidigare beroende av andra databehandlingssystem, vilka kan ligga inom ockuperat område. Av betydelse härvidlag är som redan har nämnts att en så stor del av datorkraften är koncentrerad till storstadsområdena. Vidare måste beaktas att möjligheterna att återgå till manuella rutiner fortlöpande minskar. Datoriseringen har medfört att många samhällsaktiviteter är helt beroende av en fungerande ADB-verksamhet. Det finns på flera områden inte möjlighet att utan stora svårigheter och kostnader återgå till manuella system.

Av vad jag nu har sagt har framgått att ADB-teknikens användning i hög grad bidrar till att det moderna högindustrialiserade samhället blivit alltmer sårbart. Det har också framgått att utvecklingen kan få betydande säkerhetspolitiska konsekvenser. Sårbarheten kan vara kritisk inte enbart — eller ens främst — i krigslägen utan även i situationer då hot och påtryckningar riktas mot landet. Till bilden hör också de risker som är förenade med den i världen växande terrorismen. Datorsystemens sårbarhet kan därför utnyttjas mot samhället i alla situationer från djupaste fred till krigslägen av krafter i och utanför vårt land. Dessa frågor är därför av genomgripande betydelse för samhället och därmed också för totalförsvaret.

Många utredningar och andra aktiviteter har redan beaktat en del av säkerhetsproblemen. Betydelsefulla insatser har således gjorts av överstyrelsen för ekonomiskt försvar, som bl a delvis kartlagt datoranvändningen. Statskontoret har under flera år utrett frågor om kapitalskydd, funktionsskydd, dataskydd och kvalitetsskydd. Säkerhetsfrågorna har också behandlats av dataindustriutred-

ningen i betänkandet (SOU 1974:10) Data och näringspolitik 74 och datasamordningskommittén, bl a i betänkandet (SOU 1976:58) ADB och samordning. Inom försvarsdepartementet har sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret kartlagt utvecklingen inom dataområdet och andra områden av betydelse i detta sammanhang.

Även inom närinslivet har frågorna på olika sätt behandlats av bl a näringslivets organisationer, banker, försäkringsbolag och datortillverkare.

Det bör i detta sammanhang nämnas att en prövning av datasamordningskommitténs betänkande (SOU 1976:58) ADB och samordning och remissyttrandena över detta nyss påbörjats inom budgetdepartementet. Denna prövning kan leda till nya förslag rörande styrning och samordning på ADB-området.

Trots den uppmärksamhet som hittills har ägnats säkerhetsfrågorna i samband med ADB är våra nuvarande kunskaper om säkerhetsproblemen i vid bemärkelse inte tillfredsställande. En tillräcklig överblick över dem saknas och en bättre samordning av säkerhetsfrågornas behandling måste komma till stånd. Jag finner det därför angeläget att tillsätta en kommitté med mer övergripande utredningsuppdrag. Denna bör allsidigt belysa den nya situation som har uppkommit och hur nödvändiga förbättringar skulle kunna ske. Arbetet skall även vara inriktat på framtiden och bör belysa hur sårbarhetsfrågorna skall beaktas redan vid planeringen av nya datorsystem.

Mot bakgrund av det ökade beroendet mellan samhällets olika sektorer måste arbetet inriktas på både offentlig och privat verksamhet.

Utredningsarbetet bör inledningsvis koncentreras till en kartläggning och utvärdering från säkerhetspolitisk synpunkt i vid bemärkelse. Denna utvärdering bör belysa hur utvecklingen på dataområdet påverkar samhällets känslighet för störningar och samhällets förmåga att motstå våld, skadegörelse och andra påtryckningar. Av särskilt intresse torde vara sådana frågor som rör koncentrationen av datorkraft till storstadsområden, samhällets centrala databehandlingssystem, deras interna beroende av varandra och beroendet till system på den privata sektorn samt det framtida publika datanätet. En utgångspunkt för analysen kan vara den rapport om datorerna och samhällets sårbarhet som lagts fram av försvarsdepartementets sekretariat för säkerhetspolitik och långsiktsplanering inom totalförsvaret.

Vidare bör övervägas behovet av möjlig dokumentation beträffande databehandlingssystemen och i förekommande fall huruvida det är nödvändigt och möjligt att ha tillgång till och vidmakthålla manuella rutiner vid eventuella driftstörningar.

Arbetet bör inte begränsas till persondatafrågor. Det är av vikt att kommittén även kartlägger flödet av andra data. I detta sammanhang bör även uppmärksammas i vad mån beroendeförhållanden av säkerhetspolitisk karaktär kan uppkomma vad gäller internationella databanker.

Av vad jag sagt i det föregående följer att kommitténs uppdrag endast i mycket begränsad omfattning torde komma att beröra integritetsfrågor som avses i datalagen. I den mån sådana frågor likväl behöver tas upp bör utredningen samråda med datalagstiftningskommittén (Ju 1976:05).

Arbetet skall bedrivas skyndsamt. Om kommittén finner det lämpligt kan utredningsresultaten redovisas etappvis.

2 Avgränsning av utredningsuppdraget

2.1 Begreppet sårbarhet

I SÅRKs direktiv framhålls att ADB-teknikens användning i hög grad bidrar till att det moderna högindustrialiserade samhället blivit alltmer sårbart. Vidare konstateras att sårbarheten kan vara kritisk inte enbart — eller ens främst — i krigslägen utan även i situationer då hot och påtryckningar riktas mot landet. Det framhålls även att datorsystemens sårbarhet kan utnyttjas mot samhället av krafter i och utanför vårt land i alla situationer från djupaste fred till krigslägen.

Med sårbarhet menar SÅRK i det följande såväl samhällets känslighet för störning på grund av dess struktur och näringslivets uppbyggnad som dess åtkomlighet från en motståndares sida. Sårbarheten innebär med andra ord bristande förmåga hos samhället att motstå våld, skadegörelse och andra påtryckningar. För att sårbarheten inom en samhällssektor skall betecknas som hög måste en störning av sektorns produktion medföra allvarliga konsekvenser för samhället och störningen skall kunna åstadkommas med rimliga uppoffringar för angriparen.

2.2 Säkerhetspolitiska aspekter i vidsträckt mening

SÅRKs direktiv anger en vid ram vad gäller sårbarhetssituationer. Uppdraget är ingalunda begränsat till att motverka risker i samband med beredskap och krig utan tar även sikte på andra hot och påtryckningssituationer. Som en särskild faktor nämns den ökade terrorismen i världen. Många tecken tyder på att terrorismen kommer att utvecklas ytterligare under 1980-talet. I detta sammanhang kan nämnas att det finns deltagare i den säkerhetspolitiska debatten som hävdar att konventionella krig mellan de högindustrialiserade staterna blivit omoderna bl a på grund av förekomsten av kärnvapen. I stället skulle eventuellt s k surrogatkrig — bl a en slags terrorism — föras. Surrogatkrig innebär exempelvis att olika grupper, t ex etniska, religiösa eller nationalistiska med små medel söker uppnå maximal effekt genom att angripa särskilt sårbara mål, t ex datorsystem. SÅRK har sålunda sett som sin uppgift att söka belysa sårbarhetsproblem förknippade med krigs- och beredskapssituationer, terrorism samt befarade missbruk för politiska syften. Av

speciellt intresse i detta sammanhang är att försöka klarlägga vilka tekniska möjligheter som numera kan finnas att störa eller förstöra datorer belägna på långt avstånd i andra länder.

Vad gäller sårbarhetsfrågor inom försvarsmaktens ADB-verksamhet har SÅRKs uppdrag inte ansetts omfatta den del som används för rena stridsändamål. Övriga delar av försvarets ADB-verksamhet har heller inte ansetts böra specialstuderas men har i väsentliga avseenden bedömts jämförbara med den civila sektorns verksamhet såvitt gäller sårbarhetsproblem.

Enligt direktiven skall SÅRK ägna uppmärksamhet åt såväl den privata som den offentliga sektorn. I fråga om vilka dataystem inom den civila samhällssektorn och inom den privata sektorn som är av intresse ur säkerhetspolitiska aspekter — liksom från sårbarhetssynpunkt i övrigt — är några generella avgränsningar inte möjliga. Större centrala system är allmänt sett mera i riskzonen för störningar som påverkar samhället. En del sådana system är å andra sidan av sådan art att det från totalförsvarssynpunkt är av ringa eller obetydligt intresse huruvida de fungerar eller ej. Om t ex ett reklamregister av någon anledning skulle förstöras lär det knappast få någon betydelse för samhället i stort. Ett sådant register kan emellertid, fast av andra skäl, t ex om det är ett befolkningsregister, vara intressant från totalförsvarssynpunkt.

Av stor betydelse i detta sammanhang är det alltmer ökande inbördes beroendet mellan olika datasystem. Ett system som i sig självt saknar betydelse från totalförsvarssynpunkt kan få en sådan betydelse genom att ett annat system är beroende av att det fungerar. SÅRK har därför inriktat kartläggningsarbetet bl a på datasystemens alltmer fortgående integration och beroende av varandra.

2.3 Olika sårbarhetsfaktorer

2.3.1 *Sårbarhetsfaktorernas art*

Enligt SÅRKs synsätt kan sårbarhetsfaktorerna grovt uppdelas i två huvudkategorier. Den första utgörs av olika slags angrepp utifrån, t ex krigshandlingar, terroristaktioner eller kriminella handlingar av annat slag. Till denna kategori kan även hänföras missbruk för politiska syften samt yttre katastrofer och olyckshändelser. Den andra huvudkategorin omfattar sådana sårbarhetsfaktorer som ligger mer eller mindre inbyggda i själva datorutnyttjandet. Hit räknas exempelvis datordriftens koncentration, beroendet av kompetent personal och av bistånd från utlandet, brister i fråga om dokumentation eller brister i systemvarans kvalitet. Vidare hänförs till inre sårbarhet de risker som uppkommer genom att känsliga uppgifter eller stora datamängder lagras i dataregister.

SÅRKs uppdelning av sårbarhetsfaktorerna kan inte strikt upprätthållas och ter sig därför möjligen diskutabel. Uppenbarligen föreligger ett samspel mellan de yttre och inre sårbarhetsfaktorerna. Den som utifrån vill genomföra ett angrepp mot datorverksamheten har ofta hjälp

av verksamhetens inre sårbarhet i något avseende. SÅRK anser det emellertid vara av värde att åtminstone i kartläggningsarbetet särskilja de yttre sårbarhetsfaktorerna från de inre. Uppdelningen har viss betydelse för bedömningen av vilka skyddsåtgärder som bör vidtagas.

2.3.2 *Sårbarhetsfaktorernas verkningsgrad*

Frågan om vilka sårbarhetsfaktorer SÅRK i sitt arbete skall gå in på har något berörts i anslutning till de ovan redovisade säkerhetspolitiska aspekterna. Enligt direktiven skall SÅRK arbeta utifrån ett totalförsvarsperspektiv. Redan häri måste anses ligga att de angrepp och skador SÅRK bör ta sikte på är av relativt omfattande eller ingripande karaktär för samhället i stort. Att dra några exakta gränser är dock svårt bl a på grund av att datorer används inom så olika områden och på så många olika sätt i det svenska samhället. Vad SÅRKs arbete ytterst syftar till är att finna lösningar, som skall minska datasystemens sårbarhet. Vad man då kan och vill skydda och skydda sig mot beror även på vilken tänkt krissituation man arbetar med. Säkerhetsplanering inför beredskap och krig måste se annorlunda ut än den som tar sikte på en mer fredlig situation där angreppen knappast kan få samma bredd och omfattning. Ett visst basskydd har naturligtvis värde i alla situationer. Planeringen inför krigshandlingar måste dock rimligen vara koncentrerad på att uppnå ett avancerat skydd för de delar som är av vital betydelse för samhällets möjligheter att överleva. Även i fredssituationer måste en viss gradering ske i fråga om vad man vill skydda. Man kan inte, i vart fall inte i ett öppet samhälle som vårt, skydda sig mot alla angrepp. Ser man t ex på terroristverksamhet så ligger svårigheten att skydda sig mot sådan till stor del i att angreppen praktiskt taget är omöjliga att förutse. Terroristers farlighet ligger ofta i att de kan slå till var som helst när som helst.

Då det gäller den inre sårbarheten är verkningsgraden av de olika faktorerna sannolikt lättare att mäta. Enligt undersökningar som gjorts såväl i Sverige som utomlands har hittills fel och underlåtenhet utgjort det största hotet mot ADB-säkerhet, åtminstone vad gäller kostnader för användarna.

Med utgångspunkt från direktiven och de nu redovisade synpunkterna inriktar sig SÅRK i kartläggningsarbetet på en översikt av olika sårbarhetsfaktorer. I avsnitt IV gör SÅRK en bedömning av vilka motåtgärder som kan vara motiverade.

2.3.3 *Kriminella handlingar*

Den brottslighet som primärt kan anses vara av intresse för SÅRKs arbete är av typ spionage, sabotage, skadegörelse, utpressning i politiskt syfte samt kriminella handlingar begångna av terrorister. Sådana angrepp riktade mot vitala punkter inom det datoriserade samhället kan medföra betydande störningar av samhällets verksamhet och är därför en väsentlig sårbarhetsfaktor.

Bland den hittills kända kriminaliteten i samband med datorer intar förmögenhetsbrott en dominerande ställning. Fråga uppkommer därför huruvida SÅRK bör ägna uppmärksamhet åt förmögenhetsbrott bestående i exempelvis obehöriga förmögenhetsöverföringar med hjälp av datorer.

SÅRK finner inte anledning ägna någon speciell uppmärksamhet åt sådana brott av mera ordinärt slag. Det kan framhållas att förmögenhetsbrottsutredningen (Ju 1976: 04) enligt sina direktiv har att bl a se över den straffrättsliga regleringen av s k datamissbruk. Förmögenhetsbrott med hjälp av datorer är främst av intresse från sårbarhetssynpunkt om de får sådan omfattning att hela betalningssystemet utsätts för störningar eller eljest betydande skador för samhället uppkommer. Om ett enda brott — eller ett fåtal brott — har så allvarliga konsekvenser är detta i högsta grad en sårbarhetsfråga. Vidare kan konstateras att om förmögenhetsbrott i samband med datorer skulle bli mycket frekventa och därmed svåra att bekämpa blir även detta förhållande en sårbarhetsfaktor som SÅRK har anledning att studera.

De åtgärder som kan vidtas i syfte att förebygga förmögenhetsbrott med hjälp av datorer torde vara i viss utsträckning likartade oberoende av om den befarade brottsligheten är mer eller mindre kvalificerad. Med hänsyn härtill kan de förslag som SÅRKs arbete leder fram till i någon mån vara ägnade att gagna bekämpandet även av sådan brottslighet som faller utanför den avgränsning som ovan gjorts.

2.4 Avgränsning mot integritetsfrågor

Enligt direktiven bör SÅRKs arbete inte begränsas till persondatafrågor. Vidare sägs att SÅRKs uppdrag endast i mycket begränsad omfattning torde komma att beröra integritetsfrågor som avses i datalagen. I den mån sådana frågor likväl behöver tas upp bör SÅRK samråda med datalagstiftningskommitteen (Ju 1976:05). I direktiven nämns vidare att de stora befolkningsregistren också kan utnyttjas för politiska syften. Det sägs att grupper inom och utom landet kan t ex förteckna kategorier av människor som har stor betydelse för landets administration eller försvar i syfte att sätta dem ur spel vid kriser eller krig.

Enligt SÅRKs synsätt föreligger en klar gräns mellan integritetsfrågor och sårbarhetsfrågor. Gränsdragningen bestäms av vilket intresse man vill skydda — den enskildes eller samhällets. En annan sak är att de båda intressena ibland kan sammanfalla. Som exempel härpå kan nämnas personregister som innehåller mycket känslig information rörande levnadsförhållanden. Att sådana register är integritetskänsliga är självklart. Om informationen kommer i orätta händer kan den missbrukas även till men för rikets säkerhet. Information kan t ex användas i utpressningssyfte för att nå vissa mål som är skadliga för samhället. Därför kan åtgärder till skydd för den personliga integriteten ha betydelse för totalförsvarets intressen och omvänt.

2.5 Framtidsbedömning

En väsentlig uppgift för SÅRK är att göra en kartläggning och bedömning av sårbarhetsproblematiken, inte bara såvitt gäller nuläget, utan även för den närmaste framtiden. Direktiven anger inte någon bestämd tidsperiod som SÅRK bör försöka överblicka.

Med hänsyn till den snabba tekniska utvecklingen på ADB-området är det ytterst vanskligt att göra framtidsbedömningar. Det är därför i det närmaste omöjligt att lämna förslag till åtgärder som med säkerhet är riktigt avvägda i förhållande till den situation som råder om ett antal år. Erfarenheten från exempelvis datalagens område visar att en översyn av tillämpade åtgärder blir nödvändig efter relativt kort tid. Det finns all anledning att förutse att en sådan anpassning till den framtida utvecklingen måste ske även beträffande de åtgärder SÅRK föreslår.

3 Utredningsarbetets bedrivande

3.1 Lägesrapporten

Den lägesrapport SÅRK presenterade i juni 1978 omfattar en första kartläggning av sårbarhetsproblematiken och en kort summering av SÅRKs slutsatser med förslag till vissa riktlinjer för det fortsatta arbetet.

De tekniskt inriktade kapitlen i lägesrapporten tillkom under medverkan av konsulter. Till grund för kapitel II som behandlade datatekniken och dess användning låg en rapport utarbetad av konsulten Kjell Holmström. Kapitel III som behandlade kommunikationstekniken baserades på en rapport av Teleplan AB. Båda rapporterna finns att tillgå inom SÅRKs sekretariat. Vidare har SÅRK biträtts av överdirektören Hans Rällfors vad gäller dokumentationsproblemen.

I syfte att kartlägga vissa större datoranvändares bedömningar i sårbarhetsfrågor genomförde SÅRK våren 1978 ett antal intervjuer med företrädare för myndigheter, industriföretag, kommunikationsföretag, penninginrättningar och försäkringsbolag. Dessa intervjuer gav även en överblick över ADB-verksamheten inom nämnda organisationer. Vidare har intervjuer skett med leverantörer av datorutrustning i syfte att klarlägga i första hand ADB-verksamhetens utlandsberoende. Vid ett par tillfällen har datoranvändare föredragit speciella frågor inför SÅRK.

De myndigheter och företag som på något av dessa sätt medverkat i SÅRKs arbete är följande.

ASEA AB, datamaskincentralen för administrativ databehandling (DAFA), Folksam, Försäkrings AB Skandia, Götaverken/Arendal AB, Honeywell Bull AB, Honeywell Information Services AB, IBM Svenska AB, Kema Data AB, Kommun-Data AB, Kooperativa Förbundet (KF), LM Ericsson Telefon AB, postgirot, riksförsäkringsverket (RFV), rikspolisstyrelsen (RPS), riksskatteverket (RSV), Saab-Scania AB, Saab Univac AB, SKF AB, Sparbankernas Datacentraler AB (SPADAB), Storstockholms Lokaltrafik AB (SL), Svenska Elektroniska Data AB (SEDAB), Svenska Handelsbanken, Volvo AB samt överstyrelsen för ekonomiskt försvar (ÖEF).

3.2 Remissbehandling av lägesrapporten

Genom försvarsdepartementets försorg har lägesrapporten remissbehandlats. Därvid har yttrande avgetts av följande statliga myndigheter

och kommittér. Arbetsmarknadsstyrelsen (AMS), bankinspektionen, beredskapsnämnden för psykologiskt försvar, centralnämnden för fastighetsdata (CFD), civilförsvarsstyrelsen, datainspektionen (DI), datalagstiftningskommittén (DALK), DAFA, decentraliseringsutredningen, förmögenhetsbrottsutredningen, försvarets datacentral, försvarets forskningsanstalt (FOA), försvarets materielverk, försvarets rationaliseringsinstitut (FRI), försäkringsinpektionen, justitiekanslern (JK), länsstyrelsen i Stockholms län, länsstyrelsen i Göteborgs- och Bohus län, länsstyrelsen i Gävleborgs län, länsstyrelsen i Skaraborgs län, länsstyrelsen i Kristianstads län, länsstyrelsen i Västerbottens län, miljödatanämnden, postverket, RFV, RPS, riksrevisionsverket (RRV), RSV, skolöverstyrelsen (SÖ), statens industriverk (SIND), statens järnvägar (SJ), statens lantmäteriverk (LMV), statens vattenfallsverk, statens vägverk, statistiska centralbyrån (SCB), statskontoret, styrelsen för teknisk utveckling (STU), televerket, värnpliktsverket (VPV), universitets- och högskoleämbetet (UHÄ), utredningen om ADB inom den allmänna försäkringen m m (ALLFA), överbefälhavaren (ÖB), ÖEF.

Vidare har yttrande avgetts av Centralorganisationen SACO/SR, IBM Svenska AB, Landsorganisationen (LO), Landstingsförbundet, Leverantörsföreningen Kontors- och Datautrustning, Riksdataförbundet, Saab-Univac AB, Standardiseringskommissionen i Sverige (SIS), Svenska Arbetsgivareföreningen (SAF), Svenska Bankföreningen, Svenska Dataföreningen, Svenska Försäkringsbolags Riksförbund, Svenska Kommunförbundet, Svenska Sparbanksföreningen, Sveriges Hantverks- och Industriorganisation, Sveriges Industriförbund, Sveriges Köpmannaförbund och Tjänstemännens Centralorganisation (TCO).

Med ledning av remissinstansernas påpekanden har SÅRK gjort vissa revideringar och kompletteringar inom ramen för det fortsatta kartläggningsarbetet. Detta redovisas under avsnitt 6 nedan.

3.3 Slutbetänkandets innehåll i relation till lägesrapporten

Av praktiska skäl återges i detta slutbetänkande vissa delar av lägesrapporten. Sålunda är avsnitt II Sårbarhetsfaktorer återgivet med endast mindre redaktionella ändringar. Denna teknik medför att avsnitt II kan ge intryck av att inte vara helt aktuellt. I de fall det ansetts påkallat har emellertid kompletterande uppgifter lämnats i avsnitt III av slutbetänkandet.

Genom återgivandet av de centrala avsnitten från lägesrapporten uppnår man fördelen att slutbetänkandet kan läsas fristående i förhållande till lägesrapporten.

3.4 Sekretessproblem angående utredningsmaterialet

SÅRKs arbete med insamling av material har i vissa delar berört muntliga eller skriftliga uppgifter som hos myndigheter eller företag bedömts

vara av hemlig natur. Detta förhållande har i någon mån begränsat SÅRKs tillgång till material. Såvitt SÅRK kan bedöma har utredningsresultatet emellertid inte nämnvärt påverkats härav.

Ett annat sekretessproblem är frågan i vilken utsträckning SÅRK bör offentliggöra information som kan tänkas vara tips för en angripare som vill utnyttja datasystemens sårbarhet. En strävan hos SÅRK har varit att undvika en öppen redovisning av detaljinformation beträffande vilken den nyss antydda risken skulle kunna föreligga. Vissa fakta av ömtålig natur redovisas emellertid. I dessa fall har SÅRK gjort bedömningen att uppgifterna är kända av en potentiell angripare, t ex främmande makt, medan de däremot kan vara okända eller föga uppmärksammade bland beslutsfattare och i den allmänna debatten. Värdet av en vidgad offentlig debatt och en ökad medvetenhet om sårbarhetsproblemen har därför ansetts väga tyngre än de eventuella risker som ett offentliggörande medför.

II Sårbarhetsfaktorer

4 Angrepp utifrån

4.1 Kriminella handlingar

4.1.1 *Den straffrättsliga regleringen, kriminella handlingar av intresse*

Datorerna används i allt större utsträckning som hjälpmedel inom olika samhällsaktiviteter. Den nya tekniken påverkar människornas levnads- och arbetsförhållanden och den ger även möjligheter till brottslig verksamhet av delvis ny art. De grövre brott som på något sätt har anknytning till datoranvändning faller dock som regel in under någon straffbestämmelse i brottsbalken. Det kan t ex gälla olika tillgreppsbrott, förskingring, utpressning, skadegörelse, sabotage och spioneri. I 21 § datalagen (1973:289) har dessutom intagits bestämmelser om straff för dataintrång. Dessa bestämmelser skall fånga in obehöriga förfaranden med dataregister som inte täcks av brottsbalken. Bestämmelserna tar sikte på alla slag av upptagningar för ADB oavsett om de innehåller upplysning om enskild person.

Vad gäller terrorism är detta inte någon beteckning på något självständigt brott i straffrättslig mening. Terrorism är närmast en samlingsbeteckning för verksamhet där olika sorters kvalificerade brott används som medel att nå vissa — ofta politiska — mål. Ett vanligt terroristbrott under senare år har blivit flygplanskapning (kapning av luftfartyg) något som bl a medfört skärpta straffbestämmelser för denna typ av brott såväl i Sverige som utomlands.

Störningar inom ett datasystem kan åstadkommas genom angrepp mot olika objekt inom systemet. En grovindelning av dess objekt kan göras enligt följande.

1. Angrepp mot maskinvaran, genom t ex stöld, skadegörelse eller sabotage.
2. Angrepp mot programvara, dokumentation och registerinformation genom t ex stöld, skadegörelse, spioneri, sabotage eller förvanskning av registerinnehållet.
3. Angrepp mot datakommunikationssystem genom t ex skadegörelse, sabotage eller spioneri.

4. Angrepp mot personer som är av väsentlig betydelse för driften av systemet.

Som angetts i inledningsavsnittet är det nödvändigt att bestämma vilka typer av brottsliga angrepp utredningen skall befatta sig med. Att det måste vara brott av relativt allvarlig art står klart. Men därutöver måste brottsligheten ha den inriktningen att den allvarligt stör samhället. I inledningsavsnittet ifrågasattes om inte förmögenhetsbrott, t ex obehöriga förmögenhetsöverföringar, med hjälp av datorer borde falla utanför utredningens uppdrag. Denna typ av brottslighet kan naturligtvis vara av allvarlig art. I regel torde den dock inte kunna anses som allvarligt störande för samhällsordningen i stort. Två skäl kan dock finnas att inte helt bortse från denna typ av brottslighet. För det första kan metoderna som används ha ett mer allmängiltigt intresse. För det andra kan, om denna typ av brott blir vanliga, allvarliga psykologiska effekter uppkomma. Bl a kan misstro uppstå bland allmänheten beträffande möjligheterna att uppehålla en rimlig rättsordning i landet. I detta sammanhang bör man hålla i minnet att brottslighet av denna typ ofta är svår att upptäcka och ofta kan röra stora belopp. Förmögenhetsbrottsutredningen (Ju 1976:04) skall enligt sina direktiv även ta upp frågan om behovet av straffrättslig reglering av s k datamissbruk. I direktiven för denna utredning anför justitieministern bl a följande.

> I allt större utsträckning kommer maskinella hjälpmedel såsom datorer m m till användning inom olika verksamhetsområden bl a för kontroll, bokföring och överföring av medel. Därmed har öppnats tekniska möjligheter för brottslig verksamhet av delvis ny art. I många fall bör nu gällande straffbestämmelser kunna tillämpas på de förfaranden som det här kan vara fråga om. Odiskutabelt står vi emellertid inför en utveckling som kan behöva mötas genom nya eller ändrade straffbestämmelser. Det bör vara en uppgift för de sakkunniga att närmare uppmärksamma hithörande problem. Jag vill slutligen framhålla att innehållet och omfattningen av en vidgad kriminalisering av datamissbruk påverkas av hur kontroll- och säkerhetsfrågorna löses.

I den nya bokföringslagen (1976:125) godtas att räkenskapsmaterial endast finns på ADB-medium. För att garantera insyn har dock vissa undantag härifrån gjorts. Vidare har stora krav ställts på dokumentation av ADB-systemen. I prop 1975:104 säger föredragande statsråd bl a att det måste vara ett oeftergivligt krav då automatisk databehandling används att man utan svårighet i efterhand kan följa och kontrollera hur de enskilda posterna har behandlats och vilka bearbetningar som företagits inom datasystemet. Denna princip har även kommit till uttryck i lagtexten (se 10 § bokföringslagen).

I motion 1974:1 till riksdagen tas bl a frågan om databrott upp. En av de punkter man pekar på är att revisorernas datakunnande ofta inte är tillräckligt. I motionen sägs vidare bl a följande

> Enligt undersökningar om förmögenhetsbrott i vissa industriländer har databrott endast i tio procent av fallen upptäckts tack vare företagens egen kontroll. De andra har kommit i dagen på grund av brottslingens slarv eller en oförutserbar

slump. Man måste alltså räkna med att ett mycket stort antal förmögenhetsbrott via data aldrig blir upptäckta. I en sådan situation kan inte lagstiftaren nöja sig med att konstatera att stölder, förskingringar och förfalskningar via data formellt faller under samma paragrafer i brottsbalken som alla andra sådana brott. Det måste på något sätt skapas garantier av ny art för att denna typ av brott skall kunna upptäckas och förhindras.

De brottsliga angrepp som dock är av störst intresse är av typen grov skadegörelse, sabotage, mordbrand, allmänfarlig ödeläggelse, förfalskning, spionerі och olovlig underrättelseverksamhet. Av särskilt intresse är sabotage och spionerі. I rekvisiten till dessa brott ingår just moment som tar fasta på rikets säkerhet. Straffbestämmelser för sabotage finns i bl a 13 kap 4 § brottsbalken. Den lyder:

Om någon förstör eller skadar egendom, som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket, eller genom annan åtgärd, som ej innefattar allenast undanhållande av arbetskraft eller uppmaning därtill, allvarligt stör eller hindrar användningen av sådan egendom dömes för sabotage till fängelse i högst fyra år. Detsamma skall gälla, om någon eljest, genom skadegörelse eller annan åtgärd som nyss sagts, allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel eller av anläggning för allmänhetens förseende med vatten, ljus, värme eller kraft.

Denna lagregel torde täcka en hel del av de angrepp utredningen skall intressera sig för. Vad gäller spionerі och liknande brott kan man befara att denna typ av brott kan få nya dimensioner genom datatekniken. Denna medför att allt större informationsmängder samlas på samma ställe. Information blir dessutom lättare att bearbeta och att sammanföra med annan information. I förarbetena till brottsbalken heter det bl a beträffande spionerі att ett systematiskt insamlande av uppgifter, vilka var och en för sig är ofarliga, kan vara menligt för rikets säkerhet och därför falla under paragrafen. Detta skrevs utan tanke på datateknik och den möjlighet till sammanställningar som denna ger. En form av spionerі som förmodligen kommer att bli ett allt större problem i framtiden är spionerі rörande politiska och ekonomiska förhållanden t ex s k industrispionage. Även här kan datatekniken komma att underlätta spionens arbete. En av orsakerna till detta är det ökade nationella och internationella dataflödet via olika kommunikationssystem. Spionerі av denna typ har berörts av justitieutskottet vid behandling av propositionen 1975/76:174 med följdmotioner. Propositionen innehåller förslag till ändringar i bl a bestämmelserna om spionerі. Utskottet uttalade bl a följande.

Under remissbehandlingen har rikspolisstyrelsen pekat på att det inte finns några bestämmelser om spionerі mot politiska och ekonomiska förhållanden av betydelse för rikets säkerhet och därvid hänvisat bl a till fallet Guillaume i Förbundsrepubliken Tyskland. Styrelsen finner det synnerligen angeläget att spioneribrotten blir föremål för en djupgående översyn och modernisering med hänsyn till den ändring av målinriktningen mot sådana intressen som kan skönjas i nuvarande underrättelseverksamhet. Det är enligt styrelsens uppfattning uppenbart att

bl a den politiska sektorn i svenskt samhällsliv är föremål för livlig uppmärksamhet och återkommande närmanden från främmande underrättelsetjänsters sida. — I samtliga de med anledning av propositionen väckta motionerna framställs önskemål om en sådan översyn som rikspolistyrelsen förordat. — I propositionen uttalar departementschefen i anslutning till sin redovisning av rikspolisstyrelsens uttalande att gällande spioneribestämmelser enligt hans mening ger skydd för sådana ekonomiska och politiska förhållanden vilkas uppenbarande för främmande makt kan medföra men för rikets säkerhet. — Utskottet anser för sin del i likhet med rikspolisstyrelsen och motionärerna att det beträffande sådana spionageformer, som har politisk eller ekonomisk (inkl industriell) inriktning men samtidigt faller utanför den nuvarande brottsbeskrivningen för spioneribrottet, erfordras sådana närmare överväganden som aktualiserats i lagstiftningsärendet.

Utskottets hemställan om ytterligare utredning i bl a denna fråga godtogs av riksdagen. Utredningen (Ju 1977: 04) om vissa straffbestämmelser till skydd för rikets säkerhet har av regeringen ålagts att företa den utredning som riksdagen hemställt om[1].

4.1.2 *Terrorism*

Termen terrorism används i något olika betydelser. Vad man i första hand tänker på är våldshandlingar som begås för att uppnå ett bestämt politiskt syfte. Terroristen kan då sägas ha ett ideologiskt motiv för sitt handlande. Ibland används även orden terrorism och terrorist i samband med våldshandlingar där syftet endast är att skaffa pengar.

Framställningen i det följande kommer i första hand att ta sikte på terrorism i den förstnämnda betydelsen. Terrorism är inte någon ny företeelse. I slutet av 1960-talet och i början av 1970-talet tilltog emellertid terrorismen i omfattning och fick en ökad geografisk spridning. Även Sverige berördes. Man talade om en internationell terrorism. Genom beslut den 22 september 1972 tillsatte regeringen en kommission med uppgift att överväga vilka åtgärder som borde vidtas för att förebygga politiska våldsdåd med internationell bakgrund. Kommissionens arbete låg till grund för en proposition (1973:37) med bl a förslag till lag om särskilda åtgärder till förebyggande av våldsdåd med internationell bakgrund. Lagen antogs av riksdagen och trädde i kraft under 1973. Den är nu inarbetad i utlänningslagen (1954:193). Bestämmelserna innebär bl a att utlänning som kommer till Sverige skall avvisas om det finns grundad anledning anta att han tillhör eller verkar för organisation som kan tänkas använda våld, hot eller tvång för politiska syften och det dessutom kan antas föreligga fara att utlänningen begår sådana gärningar här i landet.

För att urskilja terrorism med mera politisk inriktning har termen surrogatkrig myntats i amerikansk debatt. Termen har då syftat till att beskriva möjliga situationer i vilka utländsk makt skulle använda sig av inhemska s k terroristgrupper för att uppnå politiska mål i ett annat land, således utan att tillgripa krig. I debattskriften Krig och surrogatkrig sammanfattas den amerikanska diskussionen. Termen surrogatkrigföring kan även användas som term för sådan krigföring som smärre

[1] Utredningen har avslutat sitt uppdrag genom att i april 1979 avge betänkandet Översyn av spioneribrottet m m (Ds Ju 1979:6)

grupper för mot stater eller regeringar för att uppnå politiska mål i det egna landet eller i ett annat land. Med surrogatkrig avses alltså en sorts krigföring på lägre nivå. Enligt debattskriften riktar sig olika åtgärder inte bara, eller ens alltid främst mot regeringen eller oppositionen i det land vari de företas. De kan också rikta sig mot andra länder eftersom aktionerna ofta sker i tredje land. Avsikten är ofta att skapa en nationell eller internationell opinion. De som kan tänkas ägna sig åt terrorism eller surrogatkrigföring kan vara etniska, religiösa eller nationalistiska grupper samt politiska ytterlighetsgrupper av olika slag.

De grupper som ägnar sig åt denna typ av verksamhet försöker ofta träffa sårbara punkter för att med minimal insats uppnå maximal effekt.

De effekter man vill nå kan bl a vara att
- få publicitet för sin sak
- misskreditera och demoralisera myndigheterna
- provocera myndigheterna till överdrivna motåtgärder
- demoralisera befolkningen och minska dess tilltro till myndigheterna
- ingjuta fruktan för gruppens verksamhet.

När man diskuterar terrorism och brottsliga gärningar bör man alltid ha i minnet att angreppsobjekten ofta växlar. Detta hänger bl a ihop med att om åtgärder vidtas inom ett område som försvårar brottsliga angrepp så söker sig angriparna andra angreppsobjekt. Ett av de vanligaste terroristbrotten under senare är har varit flygplanskapning. Blir flygplanskapningar svårare att genomföra i framtiden kanske större datacentraler också kommer att höra till de angreppsmål olika terroristorganisationer väljer även om man därigenom inte spelar med människoliv. I vart fall några av de ovan nämnda effekterna kan uppnås genom angrepp mot större datacentraler eller större datasystem. Man kan t ex få publicitet för sin sak. Det kan även vara ett sätt att provocera myndigheterna till överdrivna motåtgärder osv.

Viss brottslighet, bl a terrorism har även benägenhet att smitta. Det har bl a framhållits det farliga i att terrorister lyckats väcka sympatier även bland i och för sig hyggliga laglydiga studenter särskilt i Tyskland men även i Frankrike, Italien och annorstädes. Sympatierna skulle väckts av att terroristerna för en del unga personer framstår som hjältar, därför att de är beredda att offra sina liv.

Av särskilt intresse är vissa händelser som utspelats i Italien. Där har en terroristgrupp vid minst 10 tillfällen angripit olika statliga och privata datacentraler. Det första angreppet gjordes den 26 maj 1976 då gruppen trängde in hos en lokal skattemyndighet och kastade molotovcocktails varvid åtta terminaler förstördes. Gruppen kallar sig för det kommunistiska stridande förbandet och har som motiv för sina angrepp angivit att datorer är instrument i det kapitalistiska systemet och därför måste förstöras. Flera angrepp mot datorer har därefter skett i Italien. Här finns alltså exempel på att terrorister har börjat intressera sig för datorer och dataanläggningar som angreppsmål. Liknande händelser var vanliga i USA i början av 70-talet då ett flertal datorer var utsatta för bom-

battentat och andra angrepp. Motivet var ofta protest mot Vietnamkriget.

Det kan nämnas att i Italien har under 1978 särskilda straffbestämmelser införts som reglerar angrepp mot datacentraler.

4.1.3 *Inträffade databrott*

Uttrycket databrott har i dagligt tal blivit ett samlingsbegrepp för olika kriminella handlingar. Ibland är det fråga om stöld eller något annat förmögenhetsbrott där förövaren dragit nytta av ADB-tekniken. I andra fall kan det gälla dataintrång osv.

Att databrott idag är en verklighet visas av händelser både i Sverige och utomlands. I rapporten Computer Abuse, gjord av Standford Research Institute (SRI), USA, i november 1973 diskuteras problemet databrottslighet. En katalog av inträffade fall finns även med i rapporten. Ett av de mest kända fallen rör försäkringsbolaget Equity Funding Corporation of America. 1973 avslöjades ett begrägeri till ett belopp av 2 miljarder dollar där företagets dator hade använts som ett verktyg. Bedrägeriet skedde med inblandning av företagets ledning samt vissa anställda. Fiktiva försäkringstagare skapades i datorn och falska försäkringsbrev såldes vidare till andra försäkringsbolag. Vad företaget delvis sysslade med var rena luftaffärer. De falska försäkringsbreven fick en specialkod i datorn som gjorde att revisorerna aldrig fick en verklig möjlighet att granska företagets hela bokföring.

Två fall kan hämtas ifrån en artikel i tidskriften The New Yorker 22 augusti 1977. En tysk dataoperatör lyckades komma över en mängd magnetband hos ett större företag. Banden innehöll för företaget mycket viktig information. Kopior fanns inte. Operatören begärde 200 000 dollar för att återlämna banden. Han fick vad han begärde.

Ett oljeföretag var intresserat av att köpa rätten att borra olja i Alaska. Geologer undersökte fältet för att man skulle få ett begrepp om hur mycket man högst kunde bjuda för rättigheterna. Geologisk information sändes från en terminal i Alaska till en dator vid huvudkontoret. Bearbetad information sändes sedan tillbaka till terminalen bl a med ekonomiska beräkningar. Främste konkurrenten bjöd lite mer och fick köpa rätten att borra olja. Vid undersökningar visade det sig att datakommunikationslinjen blivit avlyssnad och att konkurrenten använt informationen.

Exempel på misstänkt valfusk med hjälp av datorer anges i SRI-rapporten. Enligt Computer World 1 mars 1976 blev ett valresultat i Michigan fel på grund av omkastning av hålkort.

Enligt en artikel i den franska tidskriften Science et Connaissance, februari 1978, försvann plötsligt en anställd på en västtysk servicebyrå till Östtyskland. Med sig hade han viktig ekonomisk information om 8 000 företag i Västtyskland.

I SRIs rapport finns uppräknade flera fall där missnöjda anställda eller sådana som blivit avskedade har förstört registerinformation.

Enligt en artikel i Computer Weekly, 9 februari 1978, har två personer

dömts till sex respektive fem års fängelse för utpressning. De två hade stulit 540 magnetband och 48 skivpackar från ett av Storbritanniens största kemiska företag, Imperial Chemical Industries (ICI). Man lade beslag på såväl original som kopior. 275 000 pund var den lösensumma man begärde av företaget. ICI räknade med sex manår för att rekonstruera systemet om inte registren återställts på datamedium.

I Sverige har RPS under sommaren 1977 gjort en enkät hos de lokala polismyndigheterna för att försöka få en bild av databrott i Sverige. 30 olika fall har inrapporterats varav 29 låg i tiden efter år 1970. Det var mest fråga om förmögenhetsbrott. Bland de redovisade brotten återfanns emellertid även bombhot mot dataföretag. Vidare rapporterades ett fall av sabotage förövat genom att gärningsmannen brutit elströmmen till en datacentral. Ett fall gällde uppdatering av bilregistret med falska uppgifter. Det kan nämnas att flera fall förekommit som gäller försäljning av företags kundregister till konkurrentföretag.

4.1.4 *Sammanfattning*

Som framgått förekommer idag brottslighet av olika slag där datorer och datasystem mer eller mindre är mål eller medel för brottsligheten. Många av dessa brott är oerhört svåra att upptäcka. De brott som uppdagats i Sverige och utomlands utgör säkerligen endast en bråkdel av dem som begåtts. Många av de brott som uppdagas når heller inte offentlighetens ljus därför att den som drabbas av brottet låter bli att göra anmälan. Ett av skälen härför kan just vara att vilja undvika en publicitet som många gånger kan göra skadan mycket värre. Den ökade datoriseringen kommer även att medföra ökad databrottslighet. Den ökade användningen av ADB vid betalningstransaktioner av olika slag kan ge upphov till förmögenhetsbrott av helt nya dimensioner både vad gäller antal och belopp.

Stora datamängder, möjligheten att bearbeta dessa data, datakommunikation etc kommer att ge ökade risker för olika former av spionerі.

Datorer och datasystem har utomlands redan utgjort mål för terroristverksamhet. Den utveckling som beskrivits belägger att även i vårt land kan datasystemens sårbarhet komma att utnyttjas av krafter inom och utom landet vilka av olika skäl har intresse att åsamka samhället skada. Risken härför understryks av det faktum att terroristverksamhet av olika slag under senare år förekommit i vårt land.

4.2 Missbruk för politiska syften

Enligt vad som anges i utredningens direktiv kan samhällets sårbarhet bli kritisk inte enbart — eller ens främst — i krigslägen utan även i situationer då hot och påtryckningar riktas mot landet. Missbruk för politiska syften i form av påtryckningar och hot kan förekomma på ett flertal olika nivåer och ta sig en mängd olika uttryck.

4.2.1 *Påtryckningar och hot m m från andra länder. Förberedelse för krig*

Ett av de grundläggande elementen i den svenska säkerhetspolitiken är enligt proposition 1968:110 att vi är beslutna att vägra ge efter för påtryckningar och hot från främmande makt.

Ett tekniskt välutvecklat samhälle är i sig allmänt mycket sårbart. Därtill kommer att de västerländska industristaterna har blivit alltmer beroende av internationell ekonomi och handel samt övrigt internationellt utbyte. I det övriga utbytet ingår även dataflödet över gränserna.

Det ökade internationella beroendet kan medföra positiva effekter från säkerhetspolitisk synpunkt genom att bidra till avspänning länderna emellan. Å andra sidan blir de olika länderna känsliga för störningar i det internationella ekonomiska systemet, något som kan medföra säkerhetspolitiska risker. Hot om ekonomiska sanktioner — och ytterst förverkligande av detta hot kan framdeles bli ett vanligare påtryckningsmedel för att nå olika politiska mål. Framförallt gäller detta om den teori som förts fram på olika håll är riktig att konventionella krig mellan högindustrialiserade stater ter sig som något osannolikt.

Vårt land är i hög grad beroende av import inom datorsektorn både vad gäller material och tjänster. På grund härav kan denna sektor bli ett attraktivt objekt för angrepp, låt vara ett av flera, vid olika former av ekonomisk krigföring. Man får förmodligen räkna med att flera känsliga sektorer samtidigt kommer att beröras av dylika sanktioner.

Svenska erfarenheter från andra världskriget (t ex transsiteringsöverenskommelsen samt avbrytandet av handeln med Tyskland på grund av bl a hot om inställd leverans av naturgummi från annat land) samt öst-väst kriserna 1948—49, Kubakrisen och oljekrisen vintern 1973/74 är några exempel på hur svårt det kan vara att stå emot påtryckningar och hot.

Svårigheter att motstå påtryckningar och risk för störningar i datadriften kan uppkomma i krislägen genom reservdelsbrist. Det höggradiga beroendet av utländska tillverkare av datorer och datorkomponenter gör att redan en begränsad blockad mot import av reservdelar mycket snabbt kan få betydande effekter. Det är också av betydelse särskilt i ett krisläge att i vissa tillverkarländer betraktas dessa produkter som strategiska varor.

Beroendet av fungerande dataöverföring är stort när det gäller transmission mellan anläggningar inom landet. Vid störningar av sådan verksamhet står dock en hel del medel till förfogande för att undanröja dem. En omfattande bearbetning av data utomlands skapar ett ökat beroende. Behovet av fungerande ledningar och datorer i annans vård är påtagligt. Härtill kommer att strejker i andra länder kan förorsaka allvarliga störningar för oss. Dessutom uppkommer beroende av den politiska situationen i andra länder. Ledningar från Sverige till datacentraler i mellan- och sydeuropa passerar genom flera länder med politiska och religiösa motsättningar mellan olika grupper. Överföring av data till andra kontinenter sker bl a via satelliter, som tveklöst är att betrakta som strategiska mål för stormakterna.

Databehandling utomlands ökar förutsättningar för illasinnade grupper eller länder att utöva påtryckning genom hot om avstängning av ledningar eller tillskapande av andra hinder för svenska kunder att utnyttja utländsk dator.

Beroendet av utländsk personal för felsökning och reparation är också stort. Även om reservdelstillgången skulle vara tillfredsställande kan hot om att inte tillåta specialister att lämna service åt svenska anläggningar användas som påtryckningsmedel. Aktiva åtgärder av detta slag kan naturligtvis också ingå som förberedelse för ett angrepp men skälen kan också vara att denna personal på grund av beredskapsläge behövs i hemlandet.

I framtiden kan även tänkas situationer i vilka utländsk makt använder sig av inhemska terroristgrupper i annat land för att där uppnå vissa politiska mål. Stöd till sådana grupper måste då ske, i det fördolda, i vart fall till en början. Som tidigare nämnts kan datorer och datasystem bli intressanta angreppsobjekt för olika terroristgrupper. Är det fråga om välorganiserade grupper som dessutom har utländsk makt bakom sig kan det bli fråga om terroristaktioner som både är omfattande och sofistikerade. Att utnyttja inhemska terrorister på detta sätt kan vara tänkt som ett förberedande stadium för krigföring på högre nivå. Nästa led kan då vara gerillakrigföring eventuellt följd av intervention av den främmande staten. Terroristerna kan då bereda marken genom att utföra olika dåd bl a syftande till att demoralisera befolkningen och minska tilltron till myndigheterna. Sabotagedåd mot bl a datasystem kan försvåra det inhemska försvaret. Hot om sabotage mot bl a dataanläggningar kan användas i utpressningssyfte.

Genomgående för såväl s k låg krisnivå, hög krisnivå, säkerhetspolitisk kris eller krigssituation är behovet av fortlöpande tillgång till aktuell information. Informationskanaler, former och organisation för att snabbt sammanställa och utvärdera relevant information erfordras. Risk föreligger att genom sabotage tillgången till information begränsas eller att informationen förvanskas. Datakvaliteten är av stor betydelse.

Inför en förestående väpnad konflikt får man även räkna med att aktiviteter som spioneri och liknande brott får ökad intensitet. Infiltration bland personer med centrala uppgifter inom viktiga dataystem kan vara ett sätt att underlätta sabotage, spioneri och ge möjligheter att skapa förvirring bland allmänheten.

Risken för infiltration har hittills i någon mån mötts med personalkontroll. Dess effektivitet har alltid varit begränsad. När det gäller den tidigare nämnda utländska servicepersonalen är personalkontrollen omöjlig att genomföra. Denna internationella kategori kan bl a genom att den saknar en naturlig samhörighet med landet samt har speciella förutsättningar att åstadkomma störningar i ADB-verksamheten vara den som illasinnade i första hand försöker rekrytera.

Längre fram kommer att beröras olika befolkningsregister och register över nyckelpersoner som kan vara av stort intresse för främmande makt. Detta gäller naturligtvis framförallt inför förestående konflikter.

I 1974 års försvarsutrednings betänkande (SOU 1976:5) Säkerhetspo-

litik och totalförsvar, behandlas frågorna om försvar mot hot och påtryckningar och mot ekonomisk krigföring. I betänkandet tas dessa frågor upp från allmän säkerhetspolitisk synpunkt. Det datoriserade samhället kan inte ses som någon isolerad företeelse utan måste naturligtvis relateras till övriga sektorer och funktioner i samhället. Vad som sägs i betänkandet är därför av stort intresse för SÅRK. Vad gäller hot och påtryckningar säger försvarsutredningen bl a följande.

Supermakterna söker jämsides med avspänningssträvandena att utnyttja och skapa tillfällen att främja egna intressen, även om det skulle ske på den andra supermaktens bekostnad. Men risken för krig supermakterna emellan sätter gränser för hur långt de kan gå. Detta innebär att supermakterna strävar efter att hålla uppkommande konflikter på en låg nivå. Hot och påtryckningar kan däremot bedömas bli relativt sett mera vanliga som maktmedel i den internationella politiken.

Möjligheterna att med hot och påtryckningar tvinga svagare stater till eftergifter ugår från

- den ökande världshandeln och det allt mera internationaliserade näringslivet som å ena sidan är fredsbefrämjande men å andra sidan gör de enskilda länderna känsliga för störningar i utrikeshandeln,
- de skrämmande effekterna av moderna stridsmedel,
- de stora, komplicerade och för fysisk skadegörelse sårbara system i samhället för försörjning med t ex el, värme, vatten, transporter och livsmedel,
- möjligheterna att genom propaganda försvåra för människor att rätt uppfatta situationen.

Hot och påtryckningar kan klart utsagda eller underförstådda användas under förhandlingar för att tvinga den svagare parten till eftergifter. Den grundläggande idén är därvid att eftergifterna skall förefalla begränsade jämfört med vad som händer om de inte accepteras. Benägenheten till eftergifter kan ökas genom mer eller mindre allvarligt menade löften om förmåner. För att hotet skall nå effekt måste det uppfattas som trovärdigt. Det är emellertid alltid svårt för den svagare parten att bedöma hur långt hans motpart är beredd att gå.

Om någon av supermakerna i en mera spänd och kanske krigshotande situation i Europa finner behov av att militärt utnyttja delar av Sverige kan den söka nå målet genom förhandlingar. Dessa kan då kombineras med mer eller mindre uttalade hot om ekonomiska eller militära åtgärder om vi inte ger efter. Därvid utnyttjas osäkerheten om hotet kommer att gå i verkställighet och fruktan för följderna härav. Denna fruktan kan angriparen avsiktligt stegra genom propaganda som minskar befolkningens tilltro till den egna statsledningen och till de egna försvarsmöjligheterna och gör den benägen att finna eftergifter förmånliga.

Hot mot Sverige av begränsad omfattning kan avse stopp för leveranser av råvaror eller industriprodukter, avbrott i produktionssamarbete eller kreditrestriktioner. Ger vi trots hot inte vika kan hotet i vissa fall tänkas upptrappat till hot om vapeninsatser mot militära eller civila mål. Hotet kan också gälla ockupation av någon del av vårt land.

Har angriparen påbörjat en invasion med utnyttjande av enbart konventionella stridsmedel mot militära mål kan han tänkas hota med att övergå till bekämpning av viktiga samhällsfunktioner för att därmed bryta fortsatt försvar.

Vad gäller ekonomisk krigföring heter det bla.

Den svenska ekonomin har kraftigt internationaliserats. En större och friare marknad ger möjligheter att bättre utnyttja den internationella specialiseringens

och koncentrationens fördelar från lönsamhetssynpunkt. Utrikeshandeln har under senaste 10-årsperioden ökat från 20 % till 32 % av bruttonationalprodukten och beräknas enligt långtidsutredningen 1975 stiga till inemot 40 % år 1980. Utrikeshandeln sker nu till 80 % med OECD-länderna. Utlandets växande betydelse för vår ekonomi har bland annat visat sig genom såväl konsumtionens som produktionens ökade importberoende. Vårt ökade beroende av utländska beslutsfattare när det gäller den inhemska produktionen beror även på det utländska företagskapitalets ökade omfattning.

Produktionen kommer genom den ökade konkurrensen, de friare kapitalrörelserna samt stordriftens fördelar att koncentreras till färre enheter. Inhemska svenska företag, som tidigare var stora på den svenska marknaden, kan integreras i eller slås ut av de internationella storföretagen på den europeiska marknaden. Integrationen medför starkare och större beslutsenheter (ländergrupper i stället för länder, multinationella företag) av vilka Sverige kan bli allt mer beroende.

En fortsatt internationalisering av den svenska ekonomin medför en ökad tillgång för utlandet på ekonomiska maktmedel mot Sverige, särskilt om inflytandet koncentreras till några få stora länder eller multinationella företag. Däremot spelar i allmänhet inte det ökade svenska inflytandet inom utländska ekonomier — som också är en följd av internationaliseringen — någon stor roll på grund av dess relativt sett blygsamma omfattning.

De maktmedel som skulle kunna utnyttjas mot Sverige är

- vägran att befatta sig med svenska varor,
- avbrott i utvecklings- och produktionssammarbete,
- stopp i leveranser av komponenter och reservdelar till svensk industri,
- nedläggning av utlandsägda företag i Sverige och tillbakadragande av teknisk expertis eller
- inskränkning av leveranserna av viktiga råvaror.

Men även det omvända, nämligen att locka med särskilt förmånliga erbjudanden, skulle kunna utnyttjas.

Dessa maktmedel skulle kunna användas för att förändra maktrelationerna i Norden, framtvinga en utrikespolitisk omorientering, påverka svensk inrikespolitik eller uppnå militärt betydelsefulla favörer. De senare skulle kunna avse transitering av trupp, överflygning av svenskt område, tillgång till militära baser eller medverkan vid spärrning av Öresund.

Försvarsutredningen bedömer att sådana syften kan aktualiseras endast då mycket starka internationella motsättningar eller krig råder. Man kan räkna med att det svenska folket då är berett att acceptera betydande standardsänkningar varigenom beroendet av omvärlden minskar. Vissa åtgärder för att begränsa landets sårbarhet bör vidtas. Flera av dessa har emellertid i första hand med näringslivets struktur i stort att göra. På totalförsvaret faller främst beredskapslagring för konsumtion och produktion under avspärrning samt förberedelser för produktionsomställningar och konsumtionsregleringar.

4.2.2 *Påtryckningar och hot från olika inhemska och utländska grupper*

Påtryckningar och hot för politiska syften kan naturligtvis förekomma på lägre nivå än stater emellan. Inhemska terroristgrupper agerar ofta för att nå vissa begränsade politiska mål inom det egna landet. Det kan t ex gälla strävan efter ökad självständighet för vissa etniska, religiösa eller separatistiska grupper. Det är även vanligt att terrorister angriper mål i annat land än det mot vilket kraven riktar sig.

Erfarenheterna från t ex andra världskriget visar att infiltration kan förekomma under medverkan av alla kategorier. I dag har befolkningsstrukturen förändrats så att många har annat ursprung än svenskt. Det finns självfallet inte anledning att tro annat än att flertalet känner lojalitet med sitt nya hemland men samtidigt finns erfarenhet av att en del utsätts för påtryckningar utifrån. I ett krisläge är det naturligt att sådan påverkan i syfte att utnyttja olika personer för olovlig verksamhet förstärks.

I princip är det ingen skillnad mellan de åtgärder som kan vidtas av utländska intressen och av grupper inom landet. Oavsett vem som vill skapa kaos i samhället skulle det kunna tänkas ske på följande sätt. Driften vid datacentraler påverkas så att penningutbetalningar under en period ständigt sker med fel belopp. För att skapa ytterligare irritation bland medborgarna skulle t ex fel på liknande sätt i en samordnad aktion kunna utföras i SJs bokningsregister, bankernas och postgirots kontosystem, ransoneringssystem, system för masstest av laboratoriedata och det centrala skattesystemet.

Andra åtgärder som skulle kunna utnyttjas som hot i syfte att utöva påtryckningar skulle kunna vara att med fördröjd effekt utlösa i förväg inprogrammerade rutiner som leder till förstöring eller förvanskning av för samhället betydelsefull information.

Utvecklingen av databehandlingssystem bygger vidare på att användarna handlar på vissa förutsedda sätt. Exempelvis förutsätts att allmänheten i hög grad utnyttjar förtryckta, optiskt läsbara inbetalningskort. Det finns inga hinder mot att stora grupper av allmänheten som irriteras av någon åtgärd i samhället i en samlad aktion vägrar att utnyttja dessa blanketter och i stället sänder in för hand angivna delbelopp på flera vanliga blanketter. Redan en så enkel åtgärd skulle kunna skapa kaos vid många myndigheter eller företag. Hot om sådana åtgärder kan självfallet utnyttjas för påtryckningar.

4.3 Krigshandlingar

4.3.1 *Olika angreppsfall*

Sekretariatet för säkerhetspolitik och långsiktsplanering inom totalförsvaret (SSLP) har studerat olika internationella konflikter samt möjligt hot och angrepp i framtiden. Dessa studier har utgjort ett väsentligt underlag för 1974 års försvarsutredning. De olika angrepps- och krisfallen som används i planeringen kan i korthet sorteras enligt följande.

- angrepp med konventionella stridsmedel mot ett mobiliserat svenskt försvar
- överraskande angrepp med konventionella stridsmedel
- krig i Europa varvid Sverige är neutralt
- krig där ABC-stridsmedel utnyttjas
- kriser i omvärlden som leder till brist på försörjningsviktiga varor s k fredskriser.

Enligt försvarsutredningen skall, om Sverige utsätts för angrepp med konventionella stridsmedel, detta angrepp mötas och angriparen i det längsta förhindras att få fast fot på svensk mark. Angriparen skall förhindras att snabbt bemäktiga sig landet eller del av det. I varje del av landet skall bjudas segt motstånd. I sista hand skall motstånd göras i form av det fria kriget, vilket enligt försvarsutredningens mening bör förberedas redan i fred. Det fria kriget, som avses utkämpas av reguljära smärre förband, används av försvarsutredningen som en svensk motsvarighet till gerillakrig, partisankrig och motståndsrörelse. I sådan verksamhet deltar i regel även andra än militär personal. Beträffande försvar mot överraskande angrepp säger försvarsutredningen bl a följande.

Försvarsutredningen finner det nödvändigt att särskilt beröra frågan om överraskande angrepp mot Sverige. Därmed avses ett angrepp som inleds innan vårt försvar är färdigmobiliserat. Tillgången på militära styrkor och transportmedel i omvärlden innebär att det rent tekniskt finns förutsättningar för ett angrepp utan omfattande och för oss i god tid iakttagbara förberedelser. Å andra sidan kan militär kontroll över Sverige få värde för någotdera stormaktsblocket främst i samband med en akut krissituation eller krig i Europa. Den politiska händelseutvecklingen kan då ge oss förvarning. — En angripare kan sträva efter att inleda ett angrepp överraskande dels för att snabbare nå åsyftade mål, dels för att kunna reducera egna styrkeinsatser och förluster. Ett på så vis snabbt genomfört angrepp kan i vissa fall medföra mindre besvärande politiska konsekvenser för angriparen än ett mera omfattande anfall. För att avhålla från denna typ av angrepp bör försvaret utformas så att beredskapshöjningar och mobilisering kan ske så snabbt att vi hinner utnyttja även den begränsade förvarning som kan erhållas inför ett överraskande anfall till att förhindra att detta vinner framgång. Därigenom tvingas en presumtiv angripare till mera omfattande, tidskrävande och röjande förberedelser vilka i sin tur ger vårt försvar längre tid att utveckla full styrka. — Genom en allsidig underrättelsetjänst och genom smidiga former för beslut om beredskapsändringar skall möjligheterna till förvarning kunna tillvaratas och utnyttjas. — För att minska känsligheten för överraskande angrepp är det av stor betydelse att ledningssystem, liksom så långt möjligt övriga samhällsfunktioner, byggs upp decentraliserat. Därigenom minskas risken för att vår motståndsförmåga bryts genom punktvisa angrepp.

Beträffande totalförsvarets utformning med hänsyn till ABC-krigföring uttalar försvarsutredningen bl a följande.

— Trots kärnvapens avskräckande effekt kan man, som tidigare framhållits, inte bortse från att konflikter kan utvecklas till krig i Europa. Med hänsyn till upptrappningsrisken är det rimligt att anta att stormakterna vid en sådan utveckling åtminstone inledningsvis för kriget med konventionella stridsmedel i syfte att finna en bas för förhandlingar. Motiv för endera parten att i ett sådant krig insätta kärnvapen skulle kunna uppkomma i en situation där valet står mellan underkastelse och en upptrappning av kriget. Genom en begränsad insats av kärnvapen — begränsad såväl i fråga om antal, storlek som mål — kan en part då markera en stark beslutsamhet till fortsatt motstånd och uppmana till en lösning av konflikten genom förhandlingar. Vid de överväganden som föregår beslut om en första insats dominerar alltså den vidare bedömningen av de politiska konsekvenserna över militära lönsamhetskalkyler att slå ut olika mål. Denna uppfattning kan väntas bli mer förhärskande ju längre tiden går utan att kärnvapen används. Det

kan dock inte uteslutas att en sådan upptrappning leder till ett ohämmat kärnvapenkrig. Inte heller kan man helt utesluta möjligheten av att kärnvapen sätts in redan från början med förödande följder. Om kärnvapen skulle sättas in i Europa kan även Sverige bli utsatt för radioaktiv beläggning. — Vid utformningen av våra skyddsåtgärder måste flera tänkbara fall beaktas. Konsekvenserna i Sverige av kärnvapeninsatser i Centraleuropa och i vårt närområde bör begränsas. För att inte Sverige skall tvingas ge upp redan inför hot om kärnvapeninsatser mot vårt land bör våra åtgärder utformas så att inte insats av några enstaka laddningar rycker undan möjligheterna för fortsatt försvar. - Skulle Sverige anfallas när kärnvapen redan satts in vid krig i omvärlden kan vi inte räkna med någon särskild återhållsamhet mot svenskt område. I en sådan situation har Sverige små möjligheter att bjuda effektivt motstånd och samtidigt bevara en nationell handlingsfrihet enligt den säkerhetspolitiska målsättningen. Totalförsvarets ansträngningar i ett sådant läge måste koncentreras på att begränsa krigets verkningar och öka befolkningens och nationens möjligheter att överleva.

4.3.2 *Militära informationssystem*

Försvarsmaktens datorutnyttjande är inriktad mot en systemstruktur för datorbaserade informationssystem för både i fred och krig. Försvarets rationaliseringsinstitut (FRI) har utarbetat ett förslag till långsiktig inriktning av systemutvecklingen, FRI rapport 8/4-8403. FRI-rapporten innebär sammanfattningsvis

- Datorstöd skall utvecklas för såväl operativ/taktisk ledning som för ledning av förbandsproduktion. Systemutveckling samt utbyggnad av datakraft (antal och storlek på datorer, lokalisering av datorer samt sammankoppling av datorer och terminaler) skall ske utifrån de krav som verksamheten i krig ställer.
- Datorstöd skall utvecklas för myndigheter på central, regional och lokal nivå och skall till omfattning och utformning anpassas efter olika användares behov.
- Åtgärder måste vidtas för att hålla datorerna i drift i krig. Härvid bör datakraften spridas och system som skall verka i krig utvecklas för regional användning. Vissa datoranläggningar bör ges särkilt hög skyddsnivå.
- För att kunna utnyttja terminaler och ändrad lagringsteknik särskilt vid datorbearbetning av hemliga data måste åtgärder vidtas för skydd mot obehörig åtkomst av dessa vid överföring och lagring.
- I de fall snabb åtkomst och bearbetning av data krävs, utnyttjas speciell teknik (reelltidsteknik). Vid lagring av data skall register ordnas så att dels snabb åtkomst och bearbetning dels successiv bearbetning av stora datamängder möjliggörs (satsvis bearbetning).
- De totala driftkostnaderna skall begränsas genom att satsvis bearbetning i fred koncentreras till ett fåtal anläggningar medan övriga anläggningar utformas för reelltidsdrift med liten bemanning.
- Inriktningen både vad avser innehåll och tidsmässigt genomförande bör ses enbart som en beskrivning av trender mot önskvärda mål på 8 — 10 års sikt. Tidpunkter då målen kan nås blir enligt institutets mening beroende på de beslut, som årligen måste fattas mot bakgrund av de ekonomiska förutsättningarna.

Den 7 maj 1975 fattade regeringen beslut om att förslaget tills vidare skall utgöra principiell grund för det fortsatta utvecklingsarbetet.

Med regeringsbeslutet som grund och efter ytterligare utredningar har överbefälhavaren (ÖB) lagt fram en översiktlig informationssystem- och datakraftplan. Planen rullas årligen.

Det kan samtidigt nämnas att inom civilförsvaret planeras ett ADB-baserat informationssystem för verksamhet i krig.

4.3.3 *Civila myndigheters informationsbehandling*

Kungl Maj:t har den 27 september 1974 givit föreskrifter för statliga myndigheters planläggning av informationsbehandling i krig i sådana fall då automatisk databehandling används i fred och kan ifrågakomma i krig. Föreskrifterna, som i första hand tar sikte på civila myndigheter lyder.

1. Myndighet som enligt därom meddelade föreskrifter skall bedriva verksamhet i krig skall vid utveckling av system för automatisk databehandling på ett tidigt stadium av utvecklingsarbetet beakta de särskilda problem som kan uppkomma för myndighetens verksamhet i krig till följd av införande av system för automatisk databehandling och som inte betingas av fredstida hänsyn. Vid utveckling av datasystem, som avses för fredsbruk och som helt eller delvis skall användas också i krig, skall beredskapskraven beaktas så långt det praktiskt och ekonomiskt är möjligt.

2. Vid planläggning av myndighets verksamhet i krig bör automatisk databehandling i krig för administrativa ändamål förutsättas äga rum hos myndigheten endast för upprätthållande av krigsviktiga funktioner vilka inte till rimliga kostnader kan tillgodoses på annat sätt. Myndighet som avser att i krig utföra sådan databehandling skall upprätta skriftlig plan härför. Av denna skall framgå för vilka ändamål databehandlingen planeras, vilka anläggningstekniska, maskinella och personella resurser som behövs samt de särskilda kostnader som kan uppstå i fred för att hålla erforderlig beredskap. Framställning om medel för sådana särskilda kostnader skall göras i samband med de årliga anslagsframställningarna.
   För annan krigsviktig funktion där automatisk databehandling förekommer i fred skall planläggas övergång till annan behandling än automatisk databehandling. Vid behov får härvid ambitionsnivån sänkas.

3. Myndighet som avses i punkten 1 får i sin beredskapsplanläggning inte förutsätta att annan statlig myndighet eller annat organ skall tillhandahålla information på datamedium eller upprätthålla datordrift i krig om inte Kungl Maj:t medgivit det.

4. Myndighet, som i fred använder automatisk databehandling men i krig inte skall fortsätta därmed, skall planlägga för nedläggning av denna verksamhet på sådant sätt att den snabbt kan återupptas efter krigsslut.

5. Vid lokalisering av datorer som nyanskaffas eller i fred skall omlokaliseras skall så vitt möjligt hänsyn tas till beredskapsaspekter. I hithörande frågor har statskontoret att lämna råd beträffande tekniska problem och överstyrelsen för ekonomiskt försvar efter samråd med civilförsvarsstyrelsen att lämna råd beträffande val av lokalisering.

6. Överstyrelsen för ekonomiskt försvar samordnar och meddelar erforderliga anvisingar för beredskapsplaneringen inom totalförsvaret av sådan informationsbehandling som kräver datorstöd med undantag för samord-

ningen av planeringen mellan krigsmaktens myndigheter. I system-och datatekniska frågor lämnar statskontoret och försvarets rationaliseringsinstitut myndigheterna erforderliga råd.

Med stöd av dessa föreskrifter har ÖEF i mars 1975 utgivit särskilda anvisningar för planläggning av informationsbehandling i krig.

4.3.4 *Kommunala och privata system*

ÖEF gjorde åren 1971 — 72 en utredning om den privata och kommunala sektorns behov av och tillgång till datorer och datatjänster under beredskap och krig. Utredningen kom bl a fram till att det sannolikt skulle vara mycket svårt för många datoranvändare att gå över till manuella rutiner eller att använda andra datoranläggningar än de egna. Utredningen visade även att datoranläggningarna är starkt koncentrerade till storstadsområdena. 1975 — 76 företog ÖEF en ny inventering av datorbeståndet i landet och kunde då konstatera att den från beredskapssynpunkt ogynnsamma fördelningen i landet består.

4.3.5 *Olika angreppssituationer och deras effekter på ADB-system*

Vid ett angrepp med konventionella vapen mot Sverige får man räkna med att vissa delar av eller hela landet kan komma att besättas av fientliga styrkor. På grund av koncentrationen av datorkraft till storstadsområden kan ockupation av relativt begränsade delar av landet medföra att åtskilliga datasystem sätts ur spel och/eller kommer i fiendens händer. Koncentrationen medför även ökad sårbarhet vid bombangrepp och sabotage. Vid konventionella bombangrepp kan stora anläggningar helt slås ut. Ligger flera anläggningar inom en relativt begränsad yta finns stora risker att flera datoranläggningar sätts ur spel samtidigt.

Inom försvarsstaben, befästningsinspektionen, har den 1 oktober 1973 upprättats en skrivelse med rekommendationer för skydd av datoranläggningar. Rekommendationerna tar sikte på skydd mot andra stridsmedel än ABC-stridsmedel. I skrivelsen heter det bl a att bekämpning med bomber, raketer och robotar kan åstadkomma verkan genom

- splitter
- anslag (inträngning, genomslag och utstötning)
- luftstötvåg
- markskakning
- brand

Enligt rapporten antas de vanligaste förekommande bombtyperna vara av storleksordningen 250 — 500 kg. Ett något så när tillfredsställande skydd (skyddsklass 1) kan erhållas mot sådana bomber antingen genom att anläggningen förläggs till bergrum eller att vitala delar innesluts i splitterskyddande konstruktioner av minst 40 cm dubbelarmerad be-

tong. I rapporten uppskattas — för en anläggning som utan skydd skulle kosta 1,8 miljoner i byggnads- och installationskostnad — merkostnaden för skydd enligt skyddsklass 1 med skärmning och reservkraftaggregat uppgå till ca 53 % om planeringen sker från början och till ca 133 % om åtgärderna vidtas i efterhand.

Riskerna för sabotage ökar betydligt vid krigshot och krig. Sabotage kan utföras genom överraskande insatser av enskilda individer eller begränsade styrkor. Genom infiltration kan sabotage även utföras inifrån. Manipulationer kan göras med systemen så att felaktig information sprids.

Inför en hotande ockupation kan det även finnas skäl att undanskaffa eller förstöra datoranläggningar och olika register. En ockupationsmakt kan ha intresse av att komma över och använda själva datorutrustningen. Minst lika stort intresse torde finnas att komma över information av olika slag lagrad på datamedium.

I samband med behandlingen av olika befolkningsregister har datainspektionen pekat på de risker som i tider av politiska omvälvningar eller krig är förenade med förekomsten av många centrala personregister. Möjligheterna till bevakning, undanförsel och förstöring i tid minskar enligt datainspektionen ju flera sådan register som finns, och detta i stort sett oavsett de föreskrifter som datainspektionen och andra myndigheter kan meddela. I beslut beträffande Reader's Digest Aktiebolags befolkningsregister uttalar regeringen — sedan bolaget besvärat sig över datainspektionens beslut beträffande detta register — bl a att vad gäller riskerna vid politiska omvälvningar eller krig ankommer de därmed förenade frågorna om t ex bevakning, undanförsel och förstöring av personregister i första hand på andra myndigheter än datainspektionen.

Även om man numera har försökt hindra spridningen av befolkningsregister bl a genom ändring i datalagen torde det ändå finnas åtskilliga sådana kvar i framtiden. För övrigt finns naturligtvis intresse hos främmande makt att få tillgång till andra register än befolkningsregister. Det kan gälla register över nyckelpersoner av olika slag. Det behöver heller inte vara register med personinformation utan kan gälla register över vägar, fastigheter etc.

I lag (1961:655) om undanförsel och förstöring med diverse följdförfattningar regleras frågor av nu diskuterad art. ÖEF har samordningsansvar för planering av undanförsel och förstöring och har meddelat särskilda anvisningar härför. Någon specialreglering beträffande datorer och dataregister finns inte i författningarna. I ÖEFs anvisningar för planläggning av informationsbehandling i krig är dock intagna rekommendationer om arkivering på skyddat sätt samt i vissa fall om förstöring.

Vad gäller undanförsel av datoranläggningar torde detta ofta vara ett mindre realistiskt alternativ. Att flytta en större datoranläggning för att den skall användas på annat ställe är något som är dyrbart, tidskrävande och dessutom kräver noggranna förberedelser. Däremot kan det finnas skäl att göra en anläggning obrukbar om det kan antas att fienden kan utnyttja den för sina syften. En ren förflyttning av en anläggning för att

undvika att den faller i fiendehand är också tänkbar i vart fall vad gäller kringutrustning. Detta kan även vara ett sätt att skaffa reservdelar till andra anläggningar som fortfarande är i drift.

Att undanskaffa själva informationen lagrad på datamedier torde möta mindre praktiska svårigheter. I trängda lägen kan dock förstöring vara det enda som står till buds även om det medför stora svårigheter att i ett senare läge rekonstruera registren. Det kan finnas skäl att fortlöpande se över planeringen beträffande vilka register som bör undanföras eller förstöras vid en krigssituation. Planeringen bör omfatta både den offentliga och privata sektorn.

Datasystemens beroende av varandra ökar alltmer. Många system är beroende av information från andra system. I vissa fall hämtas informationen direkt genom terminalförbindelser. Överhuvudtaget går utvecklingen mot en allt mera ökad kommunikation mellan olika datasystem exempelvis genom dator-datorförbindelser. Utslagning av ett system får återverkningar på flera andra. Avbrott i kommunikationssystemen får vidsträckta konsekvenser. På den statliga sidan utgår man också i dag ifrån att ADB skall användas i krig endast för krigsviktiga funktioner. Även inom den privata och kommunala sektorn får man förmodligen ha en relativt låg ambitionsnivå vad gäller användning av datorer vid konventionella krig. En viktig faktor här är personalsidan. En stor del av den personal som behövs för datordriften måste användas för andra ändamål. Att ersätta inkallad personal kan ofta vara svårt eller omöjligt.

Vid ett krig i Europa får man även räkna med betydande svårigheter att uppehålla ADB-drift på grund av minskade eller obefintliga möjligheter att importera reservdelar och annan nödvändig materiel. Även möjligheterna till service från utlandet skulle minska eller försvinna. Sådana effekter skulle uppstå även om Sverige inte var inblandat i en konflikt i Europa.

Vid ett totalt kärnvapenkrig i vilket även vårt land är inblandat är frågan huruvida datorerna fungerar eller inte av underordnat intresse. Vid mera begränsade kärnvapeninsatser kan man som försvarsutredningen framhållit räkna med möjligheter till fortsatt försvar. Man bör då även kunna räkna med fortsatt datordrift i begränsad omfattning. Vad gäller användningen av kärnvapen får man även beakta den s k EMP (electromagnetic pulse)-effekten. En arbetsgrupp inom fortifikationsförvaltningen med uppgift att ta fram underlag för projektering av fortifikatoriskt EMP-skydd säger i en förberedande promemoria bl a följande om EMP-effekten.

Om man skall beskriva EMP-verkan kan det vara lämpligt att särskilja tre fall. — Det första är en yt- eller luftexplosion inom någon kilometer från marknivå där man är intresserad av verkan inom någon eller några kilometers avstånd. Denna verkanstyp är av speciellt intresse för hårda mål. — Det andra verkansfallet är en yt- eller luftexplosion på samma höjd som ovan, men där man intresserar sig för verkan på något eller några 10-tal km avstånd. Denna verkan är av intresse beträffande oskyddade mål samt utbredda el- och telesystem och i synnerhet sådana system som till en del har ledare vilka genomkorsar EMP-källområde,

nämligen området alldeles intill explosionen. — Det tredje intressanta fallet som närmast kan karaktäriseras som ett rent EMP-angreppsfall är en höghöjdsexplosion på en höjd större än 30 km, där man i första hand intresserar sig för EMP-verkan vid marknivå. Detta fall berör bl a el-, tele- och signalsystem emedan verkan kan bli synnerligen utbredd, upp till ett par tusen kilometer. — Ett fåtal höghöjdsexplosioner kan täcka hela Europa med EMP-effekten. Precisionen i explosionshöjden kan göras mycket hög. — Skadorna på ett elektriskt system kan ge sig till känna som övergående eller permanenta avbrott, kortslutningar eller karakteristikförändringar. Avledare och säkringar i tele- och elkraftsystem kan utlösas och störningar eller blockeringar av önskvärda funktioner kan uppstå. Minnesenheter i datorer kan under ogynnsamma omständigheter raderas.

NATOs överbefälhavare Alexander Haig har i ett tal varnat för att ett eventuellt angrepp från Sovjetunionen skulle kunna föregås av en osynlig EMP-blixt som skulle sätta bl a datacentraler ur funktion och därigenom skapa kaos. Ett sådant angrepp med EMP-vapen skulle förmodligen ske genom att vätebomber skulle explodera på strategiska punkter flera hundra kilometer upp i världsrymden.

EMP-effekten skulle således kunna påverka datorer i vårt land även om vi inte är direkt inblandade i ett krig. En del från beredskapssynpunkt särskilt viktiga anläggningar har försetts med skydd mot EMP-effekten genom elektrisk skärmning av lokalerna och genom anbringande av elektriska filter på ledningarna in i anläggningarna. Några enkla och billiga metoder att åstadkomma sådant skydd finns inte och det förefaller sannolikt att det av kostnadsskäl inte blir möjligt att inom överskådlig tid mer allmänt åstadkomma sådant skydd.

En allt större del av de internationella datoröverföringarna sker idag med hjälp av satellit. Dessa satellitsystem kan inte förväntas överleva en EMP-attack.

4.4 Katastrofer och olyckshändelser

4.4.1 *Definitioner, avgränsning m m*

När man talar om katastrofplanering som ett led i ADB-säkerhet tar ordet katastrof ibland mera sikte på konsekvenserna av uppkomna skador än på själva skadeorsaken. Denna kan även vara en uppsåtlig handling t ex sabotage. I skriften ADB-säkerhet — idag och i morgon, dokumentation från en konferens om ADB-säkerhet 18 — 19 november 1976 i Nynäshamn använder en författare följande definition av katastrof.

En i detta sammanhang användbar definition av katastrof kan vara när ett avbrott i driften av ADB-system får allvarliga konsekvenser för en organisations förmåga att fullgöra sina uppgifter eller behålla sin ställning (överleva) på marknaden.

Med katastrofer och olyckhändelser som exempel på yttre angrepp menas i det följande närmast oavsiktliga yttre händelser som kan få mer

eller mindre omfattande verkningar. Hit hör t ex naturkatastrofer av olika slag som ras, jordbävningar, översvämningar, orkaner och blixtnedslag. Katastrofer kan även uppstå genom att farligt gods exploderar, genom överslag i elkablar eller genom brand etc. Ofta är det väl närmast omfattningen av skadorna som avgör om man talar om katastrof eller olyckshändelse.

Med tanke på utredningens inriktning är det i första hand katastrofer av olika slag som är av intresse. Att dra någon klar skiljelinje mellan katastrof och olyckshändelse går dock inte. Det väsentliga är att det skall röra sig om yttre händelser som kan medföra avsevärd skada, sedan spelar det mindre roll vilken etikett som används. Naturkatastrofer och liknande olyckor kan både direkt och indirekt påverka verksamheten vid ADB-drift. Dels kan själva anläggningen skadas eller förstöras dels kan driften störas genom avbrott i el- och vattenförsörjningen.

4.4.2 *Katastrofer eller olyckshändelser som inträffat eller kan inträffa*

Stora naturkatastrofer har vi varit relativt förskonade från i vårt land. Sådana inträffar dock ibland. Ett exempel är rasen i Tuve i Göteborg den 30 november 1977 när stora lermassor gled ner i en dalgång. Följden blev bl a att flera människor dog och att ca 65 hus förstördes. Liknande ras inträffade i Surte år 1950. Kraftiga oväder har inträffat i vårt land. Dessa har åstadkommit stora skador på bl a el- och telenätet. Hösten 1969 uppstod svåra stormskador på bl a el- och telenät framförallt i södra och västra Sverige.

I Swedish Reactor Safety Study, Barsebäck Risk Assessment (Ds I 1978:1) gjord för energikommissionens räkning har försök gjorts att kvantifiera riskerna för radioaktiva utsläpp bl a på grund av yttre händelser som jordbävningar, stormfloder, stormvindar och flygplanskrascher. Av rapporten framgår att två lindriga jordbävningar inträffat i Barsebäcksområdet på 74 år. I rapporten bedöms riskerna för flygkrascher som jämförelsevis hög på grund av närheten till Kastrup. Ingen av de nämnda faktorerna bedöms dock i rapporten som några allvarligare risker men det framhålls att de likväl inte bör ignoreras.

Riskerna för ras, jordbävningar etc finns alltså även om riskerna är betydligt mindre än i t ex länder som Mexico, Japan etc. I Japan är det vanligt med stor reserv av datorkraft bl a med hänsyn till jordbävningsrisken. En stor procent av datoranvändarna har golv som skall öka skyddet vid jordbävningar.

Översvämningar i samband med skyfall förekommer relativt sällan i Sverige. Risker finns för översvämning i samband med snösmältning. Vanligast är dock översvämningar på grund av brister i ledningssystem och liknande. Ett speciellt fall av översvämningsrisk ligger däri att större dammar kan rämna. Vattenfallsverket har för energikommissionens räkning utrett hur stora risker det finns för denna typ av katastrofer. Enligt vattenfallsverkets utredning bedöms risken som mycket liten att en av de

fem största dammarna i Sverige skulle kunna rämna utan förvarning. Risken för katastrof är störst under byggnadstiden. I maj 1976 rasade en vattenkraftsdamm under byggnad.

I januari 1973 inträffade en explosion i några elkablar utanför Härnösand. Explosionen, orsakad av kortslutning, medförde att de flesta hushåll i Härnösand blev utan ström. Praktiskt taget hela samhället drabbades av elavbrott i större eller mindre omfattning. När alla abonnenterna efter ca tre dagar kopplades in och allt skulle återgå till det normala inträffade överbelastning på nätet så att Härnösand på nytt blev strömlöst. Under samma dag återkom emellertid strömmen till samtliga abonnenter. Driftstörningen i Härnösand föranledde Svenska Elföreningen och Centrala Driftledningens Beredskapsnämnd att tillsätta en kommitté för att analysera störningen och utarbeta de rekommendationer analysen kunde leda till. 1974 avgav kommittén rapporten Storstörningar i distributionsnät i tätorter. Beträffande möjligheterna att klara krisen i Härnösand med hjälp av reservkraftaggregat sägs i rapporten följande.

> Även om vissa, mycket lokala kraftbehov kan tillgodoses på detta sätt, så är aggregaten dock till föga hjälp i stort. Möjligheterna att med reservkraftaggregat från t ex militära enheter tillgodose ett stort kraftbortfall är således ytterst begränsade. För att tillgodose ett internt kraftbehov är det därför angeläget att man redan vid byggandet av för samhället viktiga institutioner (t ex sjukhus och skolor) förser dem med någon form av reservkraft.

I detta sammanhang kan nämnas att New York vid olika tillfällen blivit totalt mörklagt. Problem har då uppstått för olika datoranvändare. Bl a har flyg- och hotellbokningen fungerat dåligt.

Brand är något som kan medföra omfattande skador och i samband med brand kan det ibland vara befogat att tala om katastrofer. Vid en omfattande brand hos IBM (Program Information Department i New York) i september 1972 förstördes stora delar av det egna programbiblioteket, kundregister, operativsystem etc med stora förluster som följd. Genom att katastrofplaner fanns lyckades dock företaget relativt snabbt komma igång igen.

Åsknedslag kan förorsaka brand men kan även påverka elförsörjningen eller medföra andra skador.

4.4.3 *Möjliga effekter av katastrofer eller olyckshändelser som påverkar ADB-drift*

Ras eller liknande katastrofer som ägde rum i Tuve och i Surte inträffar relativt sällan. Att ett sådant ras skulle hända på en plats där en stor och viktig datoranläggning finns ter sig som något relativt osannolikt. Skulle något sådant likväl inträffa torde skadorna bli betydande och tidsödande att reparera i den mån det överhuvudtaget är möjligt. Även en flygplanskrasch på en datoranläggning ter sig som något relativt osannolikt. Placering av en datoranläggning nära en storflygplats eller vid områden med rasrisk bör dock om möjligt undvikas.

Eldsvådor och vattenskador hör till några av de vanligaste orsakerna till störningar i datordrift. Drabbas en större servicebyrå eller någon större datorcentral av omfattande brand eller vattenskador kan det bli fråga om driftavbrott som kan orsaka störningar i hela samhället.

Katastrofer eller olyckshändelser som medför avbrott i el- eller vattenförsörjningen kan ofta få mera långtgående följder än om någon enstaka datoranläggning direkt drabbas av en katastrof. Om el- eller vattenförsörjningen avbryts inom t ex hela Storstockholmsområdet drabbas en stor del av hela landets ADB-drift.

Det kan avslutningsvis nämnas att länsstyrelserna enligt 24 § brandstadgan (1974:81) svarar för planeringen av räddningstjänst vid nödlägen som kräver omfattande räddningsåtgärder enligt 12 § brandlagen (1974:80). Statens brandnämnd har i samråd med kommunförbundet under 1977 utgivit råd och anvisningar för planeringen av räddningstjänsten hos länsstyrelserna. Planeringen tar även sikte på ras, stormskador, översvämningar etc.

5 Inre sårbarhet

5.1 Innehållsmässigt känsliga register

5.1.1 *Befolkningsregistren*

Med utgångspunkt från 3 a § datalagen kan man definiera befolkningsregister som personregister vilka omfattar en betydande del av befolkningen i riket eller i område därav. 3 a § gäller från 1 februari 1977 och tillkom som ett provisorium. Datalagstiftningskommitteen (DALK) skall enligt sina direktiv bl a ta upp frågan om tillåtligheten av register som upptar stora delar av befolkningen inom landet eller inom visst område.

3 a § lyder numera

Tillstånd att inrätta och föra personregister som omfattar andra än medlemmar, anställda eller kunder hos den registeransvarige eller har annan därmed jämställd anknytning till denne får meddelas endast om särskilda skäl föreligger[1].

Bakgrunden till statsmakternas beslut om 3 a § är i korthet följande. Datalagen reglerade i sin ursprungliga lydelse inte särskilt tillåtligheten av befolkningsregister. Datainspektionen var emellertid från början restriktiv till sådana register och iakttog den principen att ingen vare sig myndigheter eller företag borde ha fler personer registrerade än vad som överensstämmer med ett aktuellt registers ändamål. Om inte denna princip kunde upprätthållas skulle många centrala personregister komma att inrättas. Inspektionen framhöll bl a att i tider av politiska omvälvningar eller krig är särskilda faror förenade med förekomsten av många centrala personregister. Man måste även, enligt inspektionen, räkna med risken under normala tider för att innehållet i befolkningsregister kan föras till utlandet.

Enligt ett avgörande år 1975 av regeringen efter besvär över beslut av datainspektionen ansågs emellertid datalagen i dess ursprungliga lydelse inte medge att personkretsens omfattning tillmättes självständig betydelse vid bedömning av integritetsriskerna i ett tillståndsärende. Det kunde enligt detta avgörande även ifrågasättas om sådana omständigheter som farhågor betingade av risken för politiska omvälvningar eller krig borde få påverka prövningen enligt datalagen.

[1] Paragrafen trädde i kraft den 1 februari 1977 och fick ändrad lydelse den 1 juli 1979.

Frågan om befolkningsregister blev föremål för debatt i riksdagen varvid riksdagen anslöt sig till datainspektionens grundprincip. Man antog vidare att vissa befolkningsregister skulle bli obehövliga eller kunna inskränkas till sitt innehåll genom inrättandet av ett samordnat person- och adressuppdateringsregister, SPAR[1].

Även om 3 a § kan bidra till att minska spridningen kommer ändock vissa befolkningsregister att finnas kvar.

Som beskrivits i SÅRKs lägesrapport är RFVs register ett av de mera omfattande statliga personregistersystemen. Det används som hjälpmedel för att administrera ett omfattande ekonomiskt trygghetssystem. Man räknar med att det fortgående reformarbetet vad gäller social trygghet kommer att medföra behov av ännu flera register hos RFV. RFVs system täcker hela befolkningen eftersom det omfattar barnbidragssystemet, sjukförsäkringssystemet och pensionssystmet. I RFVs system ingår eller kan komma att ingå ett betydande antal andra system som ofta också innehåller känslig information. Bland dessa märks system för yrkesskadelivräntor, bidragsförskott, obligatorisk arbetslöshetsersättning och socialförsäkringstillägg. RFVs system är emellertid under utredning av ALLFA-utredningen som enligt sina direktiv bl a har att bedöma möjligheten till regionalisering.

Registren inom folkbokföringen och skatteadministrationen — sedan mitten av 60-talet förda med hjälp av ADB — är av naturliga skäl befolkningsregister. Dessa register förs i dag länsvis. Länsstyrelsen i Stockholms län för dessutom ett samlingsregister över samtliga innevånare i landet. Driftmässigt är systemet förlagt till 14 regionala länsdatoranläggningar. För närvarande pågår arbete med att utveckla och införa ett nytt ADB-system inom folkbokförings- och beskattningsområdet. Det nya systemet bygger på en kombination av central och regional databehandling med en central anläggning och 21 länsdatoranläggningar. Systemet skall genomföras etappvis. Det nya systemet används i större utsträckning än det gamla som hjälpmedel vid skatteadministrationen. Den centrala registerföringen utgöres i huvudsak av ett s k arbetsregister för beskattningen. Detta omfattar i realiteten hela befolkningen. Registret omfattar samtliga skattskyldiga. Folkbokföringsregister och fastighetsregistren skall föras på länsnivå.

De av trafiksäkerhetsverket (TSV) förda bil- och körkortsregistren är också av den omfattningen att de får anses vara befolkningsregister. Vissa uppgifter i körkortsregistret, exempelvis om körkortsåterkallelse och varning är av känslig art. Det kan även nämnas att registren används för beredskapsplanering.

Hos SCB finns ett flertal befolkningsregister. Ett är registret över totalbefolkningen (RTB), som innehåller — vilket framgår av namnet — hela befolkningen. Registret innehåller dock relativt få uppgifter om varje person. Vidare finns hos SCB folk- och bostadsräkningarna från 1965, 1970 och 1975 bevarade på ADB-medium. Därutöver kan nämnas inkomst- och förmögenhetsregistret (ca 6 milj personer).

Ett annat befolkningsregister under uppbyggnad är riksdatasystemet inom exekutionsväsendet (REX-systemet). Avsikten med REX-systemet

[1] SPAR finns beskrivet i lägesrapporten på sid 67 ff.

är att det skall fungera som ett hjälpmedel i samband med registrering och handläggning av indrivningsmål. Fullt utbyggt beräknas systemet innehålla uppgifter om mer än 800 000 gäldenärer.

Register av stort intresse i detta sammanhang är de som ingår i VPVs personalredovisningssystem. Registren omfattar 1,4 miljoner människor och innehåller bl a uppgift om krigsplacering.

Det av RPS förda centrala passregistret är även ett befolkningsregister. I detta sammanhang kan nämnas att passlagen (1978:302) förutsätter att RPS i anslutning till passregistret registrerar personer som på grund av psykisk sjukdom inte får meddelas pass utan föregående s k passtillstånd (se proposition 1977/78:156).

Det ovan nämnda SPAR med DAFA som registeransvarig är delvis i drift sedan den 1 januari 1978. Syftet med registret, som omfattar hela befolkningen och innehåller vissa basuppgifter (namn, adress etc), är att kunna minska behovet av omfattande register inom såväl den privata som offentliga sektorn. Genom att olika användare kan få dessa basuppgifter från SPAR räknar man med att många kan lägga ner sina register eller krympa dem vad gäller antalet registrerade.

Bland de statliga befolkningsregister som är under utveckling skall slutligen det tidigare nämnda fastighetsdatasystemet beröras. CFD inrättades 1968 för att bygga upp detta system. Det skall användas som hjälpmedel att föra fastighets- och inskrivningsregistren. I registren skall även ingå koordinater med vars hjälp de olika fastigheterna kan lägesbestämmas. Koordinatsättningen skall underlätta samhällsplaneringen.

För att även kunna knyta rikets innevånare till de lägesbestämda fastigheterna — fastighetsägarna finns naturligtvis redan i grundregistren — har CFD framställt s k koordinatsatta personband. Detta har skett genom att de av länsstyrelsen förda kameralbanden (folkbokföringsband) har kompletterats med koordinater. Med hjälp av olika integrationsnycklar, främst personnummer, kan sedan ytterligare personuppgifter tillföras genom samkörning med andra personregister. Data kan redovisas grafiskt i form av t ex rutkartor, prickkartor och isaritmkartor.

Genom att man i fastigheten kommit ner på lägsta tänkbara administrativa nivå kan man oberoende av andra administrativa gränser som kommun, församling etc, ta fram översiktliga kartor med information beträffande praktiskt taget vilket område som helst. Det går t ex att selektera fram olika åldersgrupper inom visst område, något som kan användas vid planering av skolor, daghem, ålderdomshem etc. Detta innebär naturligtvis stora fördelar för samhällsplanerarna men samtidigt möjligheter för en angripare som vill skaffa sig kontroll över befolkningen i landet. Det är även tekniskt möjligt att med en höjdkoordinat registrera uppgifter om våningsplan m m. Koordinaterna kan även användas som hjälpmedel att rikta in olika slags vapen.

Koordinatsatta personband finns i dag beträffande flera län. I februari 1978 beslutade riksdagen att arbetet skall fortsätta med uppbyggnaden av ADB-baserade fastighets- och inskrivningsregister. Utvecklingsarbetet som dittills varit inriktat på ett integrerat system kommer att ändras. Enligt riksdagsbeslutet skall två skilda ADB-system, ett för

fastighetsregistreringen och ett för inskrivningsväsendet skapas.

Vad gäller de koordinatsatta personbanden har datainspektionen år 1975 överlämnat frågan om dessa register till regeringen (justitiedepartementet) och hemställt att regeringen beslutar om frågans vidare handläggning. Datainspektionen fann att registren i och för sig krävde inspektionens tillstånd men ansåg att registren borde prövas i ett större sammanhang med beaktande inte enbart av integritetsfrågorna utan även av samhällsplaneringens behov och en del andra faktorer som det inte ankom på inspektionen att ta ställning till. Ärendet har av regeringen avskrivits med hänvisning till att frågan kommer att behandlas av den nyligen tillsatta utredningen om den fortsatta fastighetsdataverksamheten.

Det kan nämnas att även Nordiska institutet för samhällsplanering (Nordplan) utvecklat ett samhällsplaneringsregister med personuppgifter i kombination med koordinater. Här koordinatsätts olika väg- och gatusegment. Systemet kallas NIMS (Nordiskt informationssystem och metoder för samhällsplanering).

I avvaktan på regeringens ställningstagande beträffande de koordinatsatta personbanden har flera länsstyrelser och kommuner av datainspektionen medgivits tillstånd att tills vidare föra planeringsregister med användande av koordinater både enligt CFDs och Nordplans modeller.

Även på den kommunala sidan finns register som täcker kommunrespektive landstingsmedlemmarna. Det finns t ex register för planering av sjukvården, framställning av patientkort och andra samhällsplaneringsändamål.

Inom den privata sektorn finns totalregister eller register som innehåller större delen av befolkningen hos försäkringsbolaget Folksam, hos Datema AB, som är ett serviceföretag med personregister för bl a adressuppdateringar och direkreklam och hos Reader's Digest AB som har ett eget register för reklamändamål. Vidare har UC det tidigare nämnda kreditupplysningsregistret fört med hjälp av ADB. I detta register ingår ungefär 6,5 miljoner människor. Registret innehåller relativt djup information som belyser de registrerades ekonomi. Även ABAK-JUSTITIA har ett stort kreditupplysningsregister fört med hjälp av ADB.

Hos datainspektionen hade vid utgången av juni 1977 ungefär 260 ansökningar enligt övergångsbestämmelserna till 3 a § datalagen kommit in för omprövning. De flesta avser register hos kommunerna som utgör underlag för handläggning av ärenden om bostadsbidrag. Bland övriga register av större intresse kan nämnas register hos RSV, UC, RPS, Datema AB, Reader's Digest AB, Folksam och SCB. Inspektionen har prövat några ansökningar enligt övergångsbestämmelserna. Två ärenden som lett till avslaghar överklagats till regeringen som dock inte ändrat avslagsbesluten. Datainspektionen har även med stöd av 3 a § datalagen meddelat beslut i ett antal ärenden som gäller register som tagits i drift efter den 1 februari 1977, då lagändringen trädde i kraft. Både avslags- och bifallsbeslut har givits. I en del fall har tillstånden tidsbegränsats.

Som framgår finns en mängd befolkningsregister av varierande bredd

och djup. Från sårbarhetssynpunkt ligger riskerna med befolkningsregister däri att de kan komma till stor användning även för en angripare i olika kris-och krigssituationer. Erfarenheter utomlands härav finns bl a från andra världskriget. Det finns olika sätt och olika ändamål för angripare att använda registren. Flera av dem framförallt inom den offentliga sektorn är funktionellt känsliga. Detta behandlas närmare i avsnitt 5.2.

Här skall dock nämnas att om man t ex utsätter skatteregistren, framförallt då de som är under uppbyggnad, eller RFVs register för olika störningar och manipulationer kan detta få påtagliga effekter i form av oro i samhället och misstro mot myndigheterna. Att nå sådana närmast psykologiska effekter kan ingå som ett moment i mera långtgående planer på att angripa eller omstörta samhället.

En påtaglig risk med spridning av befolkningsregister ligger däri att den underlättar möjligheterna att föra ut denna typ av register till utlandet. Visserligen finns vissa bestämmelser i datalagen och sekretesslagen som skall motverka sådana möjligheter men dessa regler torde inte räcka för att helt sätta stopp för sådana förfaranden. Om olika register förs till utlandet kan de sedan komma att användas inför och vid en krigssituation bl a i syfte att sprida propaganda eller för att underlätta kontrollen av befolkningen i erövrade områden. Ett basregister i utlandet med hela befolkningen kan t ex tänkas bli utbyggt med ytterligare information av känslig art. Att hålla ett sådant register aktuellt under någon längre tid torde dock möta vissa svårigheter.

SÅRK vill i sammanhanget peka på de möjligheter som i dag finns att ur register av totalbefolkningskaraktär "lista ut" olika kategorier av eller samtliga utländska medborgare av viss nationalitet som är bosatta i Sverige.

Den största risken ligger dock sannolikt däri att ett antal här befintliga register faller i en eventuell angripares händer. Denne skulle därigenom få ett utomordentligt instrument att kontrollera befolkningen. Framförallt gäller detta om ett flertal register skulle kunna sambearbetas. Ett särdeles utmärkt hjälpmedel för kontroll av befolkningen skulle vara de koordinatsatta personbandens utbyggda med anna personinformation. Med karteringar kunde då olika grupper av särskilt intresse placeras geografiskt på olika kartor.

Uppgifter om persondata kompletterade med information om bostads- och uppehållsort ger alltså stora möjligheter till kontroll av befolkningen inom ockuperat område. Är uppgifterna dessutom åtkomliga från terminaler i rörliga enheter torde kontrollen av befolkningens rörelser kunna bli mycket effektiv.

5.1.2 *Exempel på register som innehåller företags- och liknande uppgifter*

Vad gäller personinformation finns en i datalagen inskriven skyldighet att ange ändamålet med olika register. Motsvarande bestämmelser finns inte beträffande annan information.

Ett stort antal myndigheter t ex SIND, statens jordbruksnämnd, länsstyrelserna, RSV, naturvårdsverket, statens pris- och kartellnämnd (SPK), statens planverk samt ÖEF har rätt att inhämta i princip alla de uppgifter som de anser sig behöva för sin verksamhet. En stor del av dessa uppgifter insamlas av SCB på uppdrag av respektive myndighet utöver den uppgiftsinsamling som SCB bedriver för rent statistiska ändamål. Till följd härav och genom datateknikens utnyttjande har lagrats allt större mängder företagsdata i offentliga datasystem. I rationaliserings- och besparingssyfte sker ofta insamling av olika uppgifter från företag i ett sammanhang. Detta ökar risken för spridning av uppgifter till icke avsedd användare. Känslig företagsinformation som finns hos myndigheter är visserligen ofta sekretessbelagd men ibland försvinner sekretesskyddet när informationen lämnas till en annan myndighet.

Eftersom näringslivet är den viktigaste delen i det ekonomiska försvaret utgör förhållandet en allvarlig sårbarhetsfaktor.

Situationen belyses med följande exempel. Som ett led i uppbyggnaden av en beredskap mot miljökatastrofer i samhället pågår uppläggning av en miljödatabas, miljövårdens informatinssystem (MI). Ett projekt rör varor som kontrolleras enligt lagen (1973:329) om hälso-och miljöfarliga varor. I projektet utreds bl a ADB-rutiner för produktkontrollnämndens (PKN) register över ca 60 000 kemiska produkter och beståndsdelar som ingår i dem[1]. Tillverkare, importörer m fl är skyldiga att anmäla sådana produkter till PKN. Informationen i produktregistret är för övrigt delvis av sådan art att den kan innehålla fabrikationshemligheter bakom vilka kan ligga stora utvecklingskostnader.

Inom ett annat MI-projekt byggs ett register upp inom arbetsmiljöområdet. Ändamålet med registret är att tillhandahålla information om arbetsmiljön för tillsynsmyndigheter inom detta område. Registret innehåller stora mängder information om såväl företag som anställda.

Genom införandet av organisationsnummer har grunden lagts för att koppla samman specifika företag med produktionsförhållanden, lagertillgångar och en mångfald andra företagsuppgifter. Detta är givetvis till fördel för samhällsplaneringen men innebär samtidigt starkt ökade möjligheter för icke avsedd användning. Företagsregister av denna art finns förutom hos RSV och SCB också hos SPK vad gäller butiker och hos patentverket vad gäller patentansökningar. Vidare kan nämnas datorleverantörernas kundregister som dessutom ofta förvaras utomlands.

Sveriges industriförbund har i skrivelse den19 maj 1978 till försvarsdepartementet, vilken skrivelse överlämnats till SÅRK, tagit upp problem av nu berörd art. Industriförbundet skriver bl a följande.

> Företagens sårbarhet till följd av datateknikens utnyttjande bl a genom lagring av allt större mängder företagsdata i offentliga datasystem har enligt Industriförbundets uppfattning antagit sådana proportioner att en allmän översyn bör göras av de förutsättningar som gäller för företagens skydd. Vad nu sagts har lett till att en helt ny situation uppkommit som påverkar ekonomi och samhälle. Medvetenheten härom har på flera håll i Europa aktualiserat ny lagstiftning som omfattar inte blott persondata utan även data om juridiska personer.

[1] Antalet har senare visat sig vara betydligt större

Samhället och därmed näringslivet är beroende av fungerande kommunikationer och försörjning med elektrisk energi, vatten m m. För att tillhandahålla erforderliga tjänster används ADB i en stor och starkt ökande omfattning. Exempel härpå är följande. Inom SJ är man helt beroende av ADB för materielredovisningen och biljettförsäljningen. De moderna ställverken är helt datoriserade både för större rangerbangårdar och för styrning av vissa fjärrställverk. Redovisningen och utnyttjandet av hela vagn- och lokparken kommer att ske med hjälp av ADB.

Samtliga landets fyrar avses bli automatiserade och styras med hjälp av en centraldator.

Ett ytterligare exempel på datalagrad information av denna typ är de uppgifter om vägnätet (vägar, broar etc) som är lagrad i vägverkets databank.

Samhällets totala energiförsörjning är beroende av skilda ADB-system med en hög grad av centralisering. Systemen används som hjälpmedel vid materielförsörjning till huvudförråd och till materielbehovsställen samt för att förse arbetsplatserna med redskap vid linjebyggnation eller reparations- och underhållsarbete.

Allmänt sett kan konstateras att även blygsamma störningar kan ge stora negativa effekter för kraftförsörjningen.

Televerket är inom praktiskt taget alla delar av sin verksamhet starkt beroende av att elektronisk utrustning i växlar m m samt datorsystem för televerkets totala verksamhet fungerar störningsfritt.

Vad gäller kommunerna, i vart fall de större, förekommer en hög grad av datorisering vad gäller drift och underhåll av el, vatten, avlopp och gas. I dessa system finns en mångfald tekniska och geografiska detaljbeskrivningar.

5.1.3 *Problem med register med särskilt känslig information*

Vissa register kan innehålla så känslig informatin av personlig art att de även kan vara farliga från sårbarhetssynpunkt. Register inom t ex sjukvård och socialvård, kriminal- och polisregister etc kan innehålla uppgifter som i orätta händer skulle kunna användas för att pressa fram uppgifter av betydelse för totalförsvaret tillgängliga för någon som berörs av den känsliga informationen. Man kan naturligtvis fråga sig om datatekniken medfört några ökade risker i detta avseende. Å ena sidan har tekniken i viss utsträckning gett möjligheter till bättre kontroller och därmed ökad säkerhet. Till följd härav har risken för obehörig åtkomst av känsliga registeruppgifter generellt sett blivit mindre efter databriseringen av sådana register än den var när registren fördes manuellt. Å andra sidan har datatekniken möjliggjort lagring av betydligt större informationsmängder än som tidigare var möjligt. Även sammanföring av information från olika register sker lättare med den nya tekniken. Genom terminalverksamhet har ibland många fler fått tillgång till registerinformation än när manuella register fördes. Den ökade säkerhet som inledningsvis vanns genom att över landet utspridda konventionella register koncentrerades till mer lättbevakade centrala dataanläggningar

har i viss mån försvunnit genom terminalverksamheten. Anslutningen av terminaler från olika delar av landet till de centrala datasystemen ger nu riksåtkomst till sådan information som förr bara var tillgänglig på regional nivå.

En särskild fara ligger däri att känslig information i vissa fall sprids från register till register. Ibland översänds fullständiga kopior av register till annan myndighet. Ett exempel härpå är att till SCB lämnar andra myndigheter för statistiska ändamål omfattande information av känslig natur direkt på datamedium. Från t ex polis-, kriminal- och socialregistren och andra källor lämnas till SCB uppgifter om brottslighet, social missanpassning etc. Hos SCB sparas ofta mer material än hos myndigheterna själva. Genom att informationen sprids ökar även riskerna för att den skall hamna i orätta händer.

Känslig information som finns hos myndigheter är i regel sekretessbelagd. Emellertid kan ibland sekretesskyddet försvinna om informationen lämnas till annan myndighet. Det är inte alltid sekretessen följer med den överlämnade informationen. Samtidigt skulle en total fortplantning av sekretessen leda till att offentlighetsprincipen skulle urholkas. Sekretessbestämmelserna är dessutom ofta svårtolkade och det kan vara svårt att avgöra om sekretessskydd finns eller ej. Sålunda har t ex diskuterats om 16 § sekretesslagen i lydelse före den 1 januari 1978 var tillämplig på uppgifter som primärt insamlats för andra ändamål än statistik. Om inte samma sekretess skulle kunna åberopas som vid den myndighet som lämnat uppgiften skulle alltså känslig information helt plötsligt bli offentlig. I den ändring av 16 § sekretesslagen som trädde i kraft den 1 januari 1978 framgår det klart av lagtexten att statistiksekretessen omfattar även sådana för statistik lämnade uppgifter som ursprungligen insamlats av en myndighet för annat ändamål än statistikproduktion. I de fall ursprungssekretessen inte kan åberopas hos t ex SCB kan detta dock innebära att sekretesstiden förkortas betydligt. Statistiksekretessen är 20 år medan t ex uppgifter om begångna brott kan ha en sekretesstid på 70 år hos andra myndigheter. Ett förslag till ny sekretesslag har framlats inom justitiedepartementet (Ds Ju 1977:1 och 11). Förslaget som remissbehandlats har lett till proposition under hösten 1979 (proposition 1979/80:2).

5.1.4 *Register över nyckelpersoner*

I avsnittet om befolkningsregistren har pekats på riskerna för att dessa register skulle kunna användas som ett effektivt kontrollmedel i en angripares hand. De personer en angripare kan tänkas vilja få kontroll över är nyckelpersoner inom olika områden. Nyckelpersoner behöver inte nödvändigtvis vara enstaka personer i framskjuten ställning. Det kan även röra sig om en hel grupp eller yrkeskår där medlemmarna sammantaget har en nyckelfunktion i samhället, t ex en grupp tekniker inom ett specialområde. Sådan information kan visserligen delvis hämtas från tryckta rullor, statskalendern m m, men situationen har påtagligt förändrats. Genom utnyttjande av registerinformation kan ett väsentligt

ökat antal kategorier av personer letas fram ur aktuella register och antingen sättas ur spel eller användas för angriparens egna syften. Som exempel på register som kan tänkas användas för sådana ändamål kan nämnas värnpliktsverkets personalredovisningsystem, statens löneuträkningssystem (SLÖR), med ca 170 000 statstjänstemän och kommunernas personaladministrativa system K-PAI som lagras och bearbetas gemensamt för flertalet kommuner hos Kommun-Data AB. Men även i mera banala register av typ postens adressregister (PAR) — ett reklamregister — finns nyckelpersoner inom såväl offentlig förvaltning som på den privata sektorn registrerade. Liknande s k branschregister förs av Micro-Media AB, Directus AB m fl. Ett bolag har ett register benämnt databranschen. Registret omfattar företag med egna datorer och innehåller bl a uppgifter om nyckelpersoner inom företagens ADB-verksamhet. Många servicebyråer har specialiserat sig på medlemsregister. I vissa av dessa medlemsregister torde finnas specialister av olika slag registrerade. Detta gäller även register över prenumeranter på specialtidskrifter m m.

5.2 Funktionellt känsliga system

5.2.1 *Administrativa system inom den offentliga sektorn*

Inom såväl den statliga som kommunala sektorn finns stora system för löne- och personaladministration. Det är naturligtvis viktigt att olika ersättningar utbetalas i tid och med riktiga belopp. Kortare avbrott medför i regel inga bekymmer men med lite allvarligare störningar och avbrott kan vissa problem uppstå med försenade och felaktiga utbetalningar, brister i skatteredovisningen och i redovisningen av olika avgifter som följd. Detta gäller framförallt om reservsystem saknas. De effekter som kan uppstå är av såväl ekonomisk som psykologisk art.

Flera av befolkningsregistren måste även betrakas som funktionellt känsliga. Ett exempel är RFVs olika register. Ett stort antal personer är beroende av att utbetalningarna fungerar korrekt. I vart fall lite längre avbrott skulle ge negativa verkningar vad gäller RFVs funktioner med åtföljande missnöje och oro bland de förmånstagare som på något vis skulle drabbas.

I det nya ADB-systemet för folkbokföring och beskattning kommer, vad gäller beskattningsområdet ett register på central nivå att föras. I det centrala systemet kommer en hel del för- och efterarbeten att göras som skall underlätta den manuella granskningen vid taxeringsarbetet på lokal nivå. Detta arbete skall underlättas ytterligare genom att olika granskare har tillgång, bl a via terminal, till en centralt förd skattedatabas. Den centrala registerföringen måste således fungera rätt väl för att inte allvarliga förseningar skall uppstå i taxeringsarbetet. Med hjälp av det centrala skatteregistret kommer även skattedebitering, skatteuppbörd m m att ske.

Vad gäller det planerade ADB-baserade inskrivningsregistret ställer även detta höga krav på hög tillgänglighet, dvs att systemet kontinuerligt fungerar utan avbrott på grund av driftstörningar eller andra fel. Om arbetsbalanser och fördröjningar sker hos inskrivningsmyndigheterna medför detta snabbt olägenheter när det gäller fastighetskrediter och fastighetsomsättningen.

Att VPVs system fungerar är en förutsättning för att inkallelser etc skall kunna sändas ut vid rätt tidpunkt.

Inom polisens verksamhet utgör systemen för ledningscentraler i Stockholm och Göteborg exempel på funktionellt känsliga system.

Vad gäller landstingen kan vissa patientadministrativa system vara av funktionellt känslig art. Ett av landstingen har t ex ett on-line system där huvudmålet är att kunna följa en patient hela vägen genom ett ärende om sluten vård, med remissförfarande, platsbokning, inskrivning, förflyttingar, utskrivning, diagnosrapportering, ekonomiska rutiner och rapportering till försäkringskassa.

5.2.2 *Administrativa system inom den privata sektorn*

Försäkringsbolag, kreditinrättningar m m

Banker och försäkringsbolag använder sig i stor utsträckning av datorer för administrativa ändamål. Det är då inte enbart fråga om löne- och personaladministrativa rutiner utan även om rutiner som rör försäkrings- respektive bankverksamheten som sådan.

Vad gäller försäkringsbolagen så används ADB vid administration av såväl sak- som personförsäkring. Flera av de större försäkringsbolagen har omfattande terminalsystem med terminaler på lokalkontoren. Försäkringsbolagens system är rätt känsliga för störningar. En av de känsligare delarna kan förmodas vara de rutiner som rör utbetalningar av pensioner och livräntor.

De flesta spar- och affärsbanker använder sig idag av ADB. Flertalet har dessutom omfattande on-line system. SPADAB sköter servicen för 125 sparbanker vilket täcker i stort sett hela sparbanksidan. Hos de svenska sparbankerna finns ca 3 000 terminaler. Flera av de större affärsbankerna har vardera över 1 000 terminalanslutningar. Nedanstående tabell redovisar prognoser på antalet installerade bankterminaler fram till 1980.

	Antalet installerade bankterminaler (QSC)	(SIND)
1975	6 600	
1976	7 500	
1977	8 500	8 700 (mitten av 1977)
1980	11 900	11 800

Källa: Quantum Science Corporation, SIND
Anmärkning: SINDs beräkningar bygger på uppgifter från såväl leverantörer som användare

En omfattande registrering sker inom bankväsendet av olika betalningstransaktioner, in- och utlåning etc. Ett stort informationsutbyte sker mellan bankerna — även på datamedium — och mellan bankerna och kunder av olika slag. Vidare utväxlas information mellan bankerna och närliggande företag som UC, Värdepapperscentralen (VPC), Bankgirot etc. Uppräkningen är ingalunda uttömmande.

Även bankgirot och postgirot använder sig av ADB och över dessa institut sker mycket omfattande betalningstransaktioner både antals- och beloppsmässigt. Större företag redovisar sina betalningsuppdrag på magnetband och får från giroinstituten tillbaka redovisning på samma medium. Även transaktioner on-line är möjliga.

Till följd av bankväsendets långt gångna datorisering är stora delar av det ekonomiska livet i samhället beroende av att bankernas datasystem fungerar. Avbrott i de datoriserade betalningsströmmarna skulle alltså snabbt medföra stora olägenheter inte bara för bankerna själva utan för samhället i stort.

Varuhandel

Inom varuhandeln används ADB för olika personaladministrativa rutiner. Vidare används ADB som hjälpmedel för lagerhållning, lagerredovisning, lagerstyrning, distribution etc. Med hjälp av ADB kan varor snabbare och effektivare slussas från fabrik till konsument via grossister och detaljister. Det pågår även arbete som syftar till att underlätta kommunikationen mellan de olika leden i varudistributionen. Bl a arbetar man med att få fram en gemensam varukod på dagligvaruområdet.

En av de stora fördelarna med användning av datorer som hjälpmedel för lagerhållning är att lagren därigenom kan krympas betydligt vilket i sin tur minskar behovet av lagerutrymmen. Dessa effekter ökar å andra sidan sårbarheten.

Distributions AB DAGABs datoranvändning beskrivs i SCBs promemoria 1976:11 ADB och arbetskraften — varuhandelns ADB-förhållanden, på följande sätt.

Företaget DAGAB har en mycket stor genomströmning av varor. Varje dag passerar många olika artiklar och stora mängder av varje artikel genom företaget. Man har också en stor daglig betalningsström som består av dokument av olika slag och pengar. Kravet på snabbhet är mycket stor då man bara sysslar med dagligvaror. På DAGAB arbetar man med hjälp av ett integrerat datasystem kallat System 75. — Man har en central dataenhet med terminaler ute vid lagercentralerna som är kopplade via telenätet till datorn. Om några år är det dags att byta till ett nytt system med bättre ordertagningsteknik och dataservice åt kunder, men det nuvarande har den fördelen att det inte är särskilt kostnadskrävande. — Via lagercentralerna görs beställningar av varor på terminalerna. Från datorn levereras underlag för beställningarna till inköparna i form av datorproducerade inköpslistor med försäljningsstatistik, lagerställning, uppgifter om pågående och planerade kampanjer m m. Även orderbehandlingen och faktureringsrutinerna är datoriserade. Dessutom är många av DAGABs kunder anslutna till s k automatiskt bankgiro. En stor del av betalningen går via detta och man använder magnetband som innehåller kundernas betalningssignaler och dessa skickas varje dag från datacentralen till bankgirocentralen. — För att klara av den varuström

och betalningsström man har i dag inom företaget är ADB-användning nödvändig för DAGAB om man inte vill ändra sin målsättning. Man anser det vara omöjligt att utföra rutinerna i distributionssystemet manuellt med kraven på exakthet och snabbhet fortfarande uppfyllda.

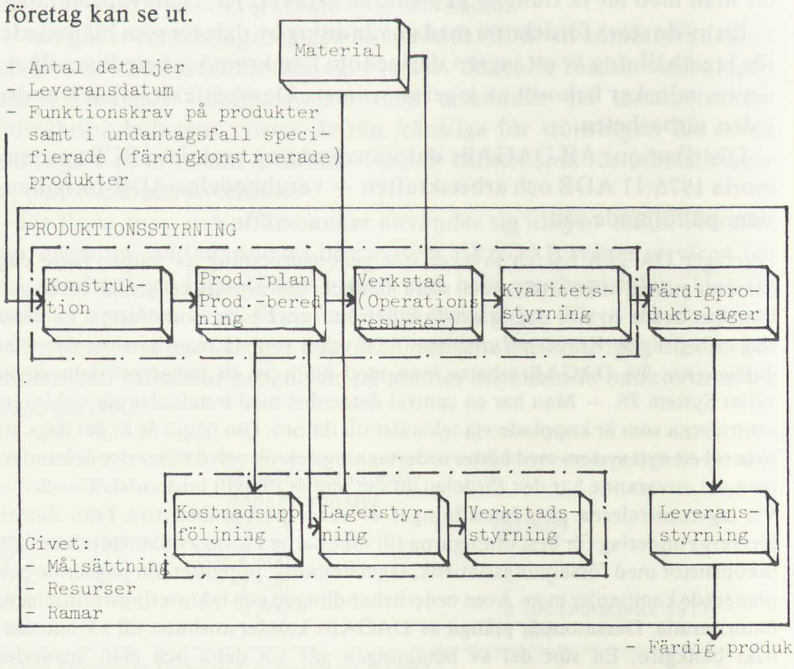
Bland några av de stora datoranvändarna på detaljhandelssidan kan nämnas Åhlén & Holm AB och KF. Vad gäller KF representerar detta företag även partihandels- och industriledet.

De tidigare lagren har ersatts av leveranser av rätt vara i rätt mängd vid rätt tidpunkt enligt schema som framställs som ett resultat av rapportrutiner från t ex en koncerns olika verksamhetsgrenar. Detta medför en beroendesituation. T o m mindre fel i datasystemet kan föranleda varubrist och produktionsstörningar.

Tillverkningsindustri

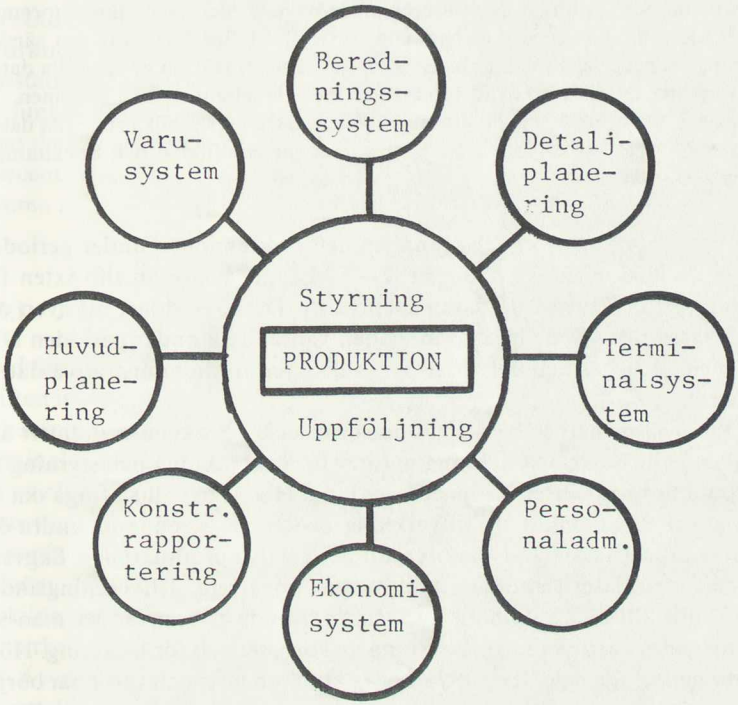
Inom tillverkningsindustrin finns olika administrativa ADB-rutiner som order, fakturering, lagerhållning, redovisning, personaladministrativa system etc. I system för produktionsstyrning används många av de uppgifter som ingår i de administrativa systemen.

Med produktionsstyrning menas att datorerna tas till hjälp vid planering och tillverkning av olika produkter. Det kan gälla såväl övergripande planering som detaljplanering. I samband med att en order kommer in kan man t ex kontrollera om och var det finns maskinkapacitet, om det finns utgångsmaterial i lager, huruvida det finns nödvändiga verktyg etc. Nedanstående figur visar schematiskt hur produktionsstyrning i ett företag kan se ut.



Källa: Samordnad datorstödd produktion — verkstadsindustrins framtid, Gunnar Kullberg m fl

Ett av de företag som intervjuats av SÅRK framhöll att deras produktionsstyrningssystem var helt integrerat med de olika administrativa systemen. Integrationen framgår av följande skiss.



Att olika system av denna typ kan vara funktionellt känsliga visas bl a av att flera företag vid intervjuerna bedömt att de redan efter kort tid skulle få svårigheter att hålla sysselsättningen i gång. I ett fall skulle svårigheter uppstå att få fram order till verkstäderna. Vid ett annat företag var man i hög grad beroende av att inköpssystemet fungerade bra.

5.2.3 *Speciella datorsystem för processtyrning m m*

Med speciella icke administrativa datortillämpningar avses tillämpningar för t ex processtyrning — styrning av verktygsmaskiner, sågar, symaskiner m m — styrning av tele-, landsvägs-, järnvägs- och sjöfartstrafik — larm och övervakningssystem etc.

Beträffande dessa tillämpningar sägs i SINDs rapport bl a följande

Datorer för speciella tillämpningar har kommit till användning betydligt senare än de administrativt inriktade datorerna. Först efter 1969 började de speciella

datorsystemen få en vidgad spridning och under 1970-talet har tillväxten för dessa system varit mycket snabb. Enligt vissa bedömningar är tillväxten för de speciella datorsystemen i storleksordningen tre gånger större än den totala datormarknaden. Denna bedömning har en relativt god överensstämmelse med de tillväxttal som SIND beräknat. Den snabba tillväxten av datorer för speciella tillämpningar torde framför allt förklaras av utvecklingen på halvledar- och mikrodatorområdet. Mikrodatorns ringa kostnad samt stora flexibilitet har gjort den särskilt lämpad för speciella tillämpningar. — Den snabba tillväxten av speciella datorsystem har medfört en ökad integration med de administrativa systemen. De senare hanterar de förras programbibliotek, synkroniserar olika speciella datorsystem, svarar för driftstatistik, kontrollerar materialflöden och beställningar m m.

Enligt rapporten visar försäljningen och produktionen under perioden 1974 — 1976 en tillväxt som är 2 — 3 gånger högre än tillväxten för administrativt inriktade datamaskinvaror. Det sägs vidare att även om tillväxten i de speciella datorsystemen väntas avta under perioden 1976 — 1980 så ligger den betydligt över tillväxten för administrativa datorsystem.

Inom järn- och stålverk, pappersbruk och petrokemisk industri används i allt större utsträckning datorer för övervakning och styrning av produktionsprocesser, s k processtyrning. Här är det alltså fråga om en långt driven automation i tillverkningsprocessen. Även inom andra delar av industrin används datorer alltmer i själva produktionen. Sågverk förses med datoriserade sorteringsutrustningar etc. Tillverkningsindustrin blir allt mer automatiserad. Inom bilindustrin använder man sig t ex av industrirobotar för svetsning av karosser och för lackering. Högautomatiserade lager för plockning av komponenter och varor har börjat användas. Redan idag skulle många arbetare kunna ersättas av industrirobotar inom t ex bilindustrin. En integrering mellan administrativa system, produktionsstyrningssystem och datorstyrda maskiner sker och kommer med säkerhet att öka.

Vad gäller kommunikationsväsendet används datorer bl a som hjälpmedel för bokningar och liknande. Det är då närmast fråga om administrativa rutiner. Dessa system kan vara känsliga för störningar. Flygbolagen t ex är i hög grad beroende av att kontinuerligt veta hur beläggningen i de olika flygplanen ser ut. Datorer används även i stor utsträckning för färdplanering, lastplanering etc.

Man räknar med att datorsystem alltmer kommer att användas för trafikövervakning och trafikledning. System för trafikflyget är redan i drift eller under installation. Det är sannolikt att likartade system under 1980-talet kommer att införas även för sjöfarten och på vissa håll även för vägtrafiken.

Även navigering och styrning av flygplan, fartyg och så småningom även bilar kommer alltmer att datoriseras. Sålunda kommer de beräkningar som fordras för fartygsnavigation på världshaven med hjälp av satelliter att bli så komplicerade att datorberäkningar fordras. Även de beräkningar som behövs för mera kustnära navigation med radiohjälpmedel kan med fördel datoriseras.

5.3 Koncentration

Vid ett försök till bedömning av vårt samhälles sårbarhet finns vissa företeelser som måste ägnas särskild uppmärksamhet. En av dessa företeelser är den ökade koncentrationsgraden av viktiga samhällsfunktioner. Inom just datorområdet finns en stark tendens till geografisk koncentration. Databehandlingen har i stor utsträckning koncentrerats till storstadsområdena, främst Stockholmsområdet. Vidare kan man tala om en funktionell koncentration vad gäller datorer och databehandling. Med detta avses närmast uppbyggnad av stora centrala system eller att koncentrationen sker genom att en mängd kunder vänder sig till en och samma servicebyrå.

5.3.1 *Funktionell koncentration*

Med funktionell koncentration menas här att stora vitala delar av datordriften inom en viktig sektor eller viktiga sektorer är koncentrerad till ett och samma ställe. Att man ibland med hjälp av datakommunikation och terminaler decentraliserar vissa funktioner som datafångst, och utskrifter av olika slag påverkar knappast bilden från sårbarhetssynpunkt. Om man t ex ser på systemet inom den allmänna försäkringen finns den centrala datoranläggningen i Sundsvall. För att ge försäkringskassorna tillgång till registrerade data och för registrering av nya data har två, åtskilda datanät byggts upp för datakommunikation. I dessa nät ingår f n cirka 1 000 terminaler. Liknande struktur har bil- och körkortsregistret. Även på den privata sektorn t ex på bank och försäkringssidan finns likartade system. Inom tillverkningsindustrin finns det exempel på starkt centraliserad datordrift. Servicebyråer med koncentrerad drift för hela koncerner är en variant på detta tema. Nästan hela sparbanksidan har sin ADB-verksamhet hos SPADAB, som i huvudsak har sin verksamhet förlagd till en datacentral. En privat servicebyrå med datordriften i huvudsak på ett ställe har ca 30 000 kunder. Inom den kommunala sektorn har flertalet kommuner sin databehandling förlagd till Kommun-Data AB som har datoranläggningar på tre orter i landet med huvudanläggningen i Stockholm. Även flera landsting anlitar Kommun-Data.

DASK, vars grundläggande uppgift var att belysa möjlig samordning inom ADB-området, har även behandlat frågor som rör centralisering, decentralisering och regionalisering.

I DASKs betänkande sägs att datordriften för den administrativa databehandlingen i större organisationer och förvaltningssektorer i allmänhet varit centraliserad till en gemensam datacentral och ofta till samma dator.

Fyra olika tänkbara alternativ för datorkraftstruktur diskuteras av DASK. Dessa är central blandad drift, regional blandad drift, regional specialiserad drift och central specialiserad drift. Uppdelningen har illustrerats med följande figur.

	Centraliserad datordrift	Regionaliserad datordrift
Gemensamma datacentraler	Ruta 1: *"Central blandad drift"* (Ett fåtal mycket stora datacentraler)	Ruta 2: *"Regional blandad drift"* (Regionaliserad datordrift med ett antal regionala datacentraler som är gemensamma för flera förvaltningssektorer)
Myndighets- och sektorsvisa datacentraler	Ruta 3: *"Central specialiserad drift"* (Nu dominerande organisation)	Ruta 4: *"Regional specialiserad drift"* (Regionalt spridd datordrift i varje förvaltningssektor för sig)

DASK behandlar även datakraftstrukturen utifrån olika säkerhetsaspekter. I fråga om lämpligheten från försvarssynpunkt m m uttalas bl a att de försvarsaspekter som är av intresse i detta sammanhang avser kraven på att datordriften organiseras på ett sådant sätt att ADB-tillämpningar i önskvärd grad är användbara även i beredskaps- och krigssituationer, att förstörelse och andra former av sabotage försvåras och att det blir omöjligt eller avsevärt försvårat för främmande makt att vare sig i fred eller krig få tillgång till data av väsentlig betydelse från försvarssynpunkt. Vidare framhålls att den försvarsbetingade säkerheten anses ställa krav på bl a geografisk spridning av datacentraler och datoranläggningar och kompatibilitet i datorutrustningen för att därigenom ge tillgång till reservanläggningar, regional uppdelning av datordriften för system som används i flera regioner samt planläggning av förfarandet vid övergång till administrativa rutiner utan databehandling. Med tanke på de av regeringen den 27 september 1974 meddelade föreskrifterna anses dock att man inte bör räkna med att administrativ databehandling i krig skall användas i samma omfattning och med samma avancerade teknik som i fredstid. Det finns därför inte skäl att med hänsyn till försvarsaspekterna generellt förorda regionalisering av datordriften för den administrativa databehandlingen i statsförvaltningen. DASK förordar i stället att man i varje särskilt fall bör ta erforderliga hänsyn till försvarsaspekterna och om tungt vägande skäl då talar för regionalisering bör en sådan lösning väljas.

Vad gäller riskerna för sabotage mot datoranläggningar och katastrofer av olika slag blir konsekvenserna av ett eventuellt sabotage mer omfattande i alternativet med ett fåtal mycket stora datacentraler — central blandad drift — än vid nuvarande datorkraftstruktur däremot mindre i alternativet regional specialiserad drift. Mellan nuvarande struktur och alternativet regional blandad drift går det inte att generellt göra jämförelser. Det bör enligt DASK gå att åstadkomma ett rimligt skydd mot sabotage i alla här aktuella alternativ bl a mot bakgrund av att det i flera avseenden kan vara enklare och billigare att effektivt skydda ett fåtal stora datacentraler än många relativt små.

DASKs slutsats vad gäller centraliserad eller regionaliserad datordrift utifrån säkerhetsfrågorna är den att de alternativ som bygger på regionaliserad datordrift inte entydigt syns vara fördelaktigare än nuvarande datorkraftstruktur utom från försvarssynpunkt. Även försvarsaspekterna bör dock till stor del kunna tillgodoses inom nuvarande datorkraftstruktur bl a genom att datacentralerna inte lokaliseras till samma ort utan förläggs till olika platser.

Vid SÅRKs intervjuarbete har framkommit att de flesta av de tillfrågade användarnas system är funktionellt koncentrerade. I något fall framhölls att detta inte föranletts av organisatoriska skäl — om så varit fallet skulle en spridning av datorkraften skett — utan snarare av hänsyn till ekonomi och tillgängliga tekniska lösningar. Några menade å andra sidan att det även av organisatoriska skäl var lämpligast med koncentrerad drift.

Ett flertal med centraliserad drift ansåg att det kunde ligga betydande fördelar, bl a från sårbarhetssynpunkt, i att på något sätt sprida datordriften. En användare som planerat ytterligare koncentration av datordriften hade efter överväganden främst från sårbarhetssynpunkt bestämt sig för att i vart fall inte gå längre i fråga om koncentration. Många räknade med att de tekniska och ekonomiska förutsättningarna helt höll på att ändras på ett sätt som skulle underlätta och göra sådan spridning fördelaktig på flera sätt. För ett flertal innebar detta att i den framtida planeringen vägdes in strukturer som i någon form skulle medföra en större spridning av datorkraften. I dessa överväganden fanns givetvis även sårbarhetsaspekterna med. En användare påpekade dessutom att sårbarhetsfrågor och ekonomi av olika skäl i hög grad hänger samman. Som skäl nämndes bl a att man blivit allt mer beroende av att datordriften fungerar vilket i sin tur medfört att man blivit tvungen att lägga ner väldigt stora summor på säkerhetsåtgärder av olika slag för att skydda sin anläggning, ett behov som även accentuerats genom att nya hottyper dykt upp som t ex terrorism.

På senare tid har talats allt mer om distribuerad datakraft. Här kan man tänka sig olika hierarkiskt uppbyggda system med två eller flera nivåer med mer eller mindre utbyggda kommunikationsmöjligheter både i höjd- och i sidled. Ett sätt att ge viss spridning av datorkraften är att använda intelligenta terminaler. Något som håller på att utvecklas är nätstrukturer där ett antal datorer är sammanbundna med hjälp av avancerade datakommunikationslösningar. Om en bearbetning inte kan ske i den närmaste datorn på grund av bristande kapacitet eller avsaknad av lämpliga program eller data skall bearbetning kunna ske vid en av de andra datorerna. Olika kombinationer kan vidare tänkas. Mera avancerade nät av nu skisserad art är ännu inte någon realitet men ligger å andra sidan inte särskilt långt fram i tiden. Flera leverantörer håller på att arbeta fram maskiner och system som skall kunna användas på detta sätt och åtminstone dellösningar är på väg. Det ökade utbudet på billiga smådatorer av olika slag underlättar naturligtvis en spridning av datorkraften. Den snabba utvecklingen på datakommunikationssidan är även en faktor av stor betydelse i detta sammanhang.

Enligt SÅRKs mening är det av stort intresse att notera att den tekniska utvecklingen fortsätter i sådan riktning att en spridning av datorkraften underlättas. En spridning av datorkraften har betydande fördelar från sårbarhetssynpunkt, såväl vad gäller en krigs- och beredskapssituation som under normala förhållanden.

Utslagningen av en större viktig datacentral kan få förödande verkningar. Det kan visserligen vara lättare att effektivt skydda ett fåtal stora datacentraler än många relativt små mot sabotage och andra former av utslagning. Att skydda en större central är dock något som är mycket kostsamt. Även om man vidtar många och dyrbara skyddsåtgärder räcker dessa förmodligen ändå inte till vid en väl planerad terroristaktion. Man har också svårt att skydda sig effektivt mot angrepp som kommer inifrån den egna organisationen. Går man in för mindre enheter finns heller inte samma intresse av att störa dem eftersom effekten blir begränsad. Behovet att skydda dem minskar även därmed.

5.3.2 *Geografisk koncentration*

I direktiven för SÅRK framhålls att databehandlingen är starkt koncentrerad till storstadsområdena. Detta förhållande belyses i SINDs rapport enligt vilken 62 procent av datorerna och inemot 75 procent av terminalerna i slutet av 1975 fanns hos företag eller institutioner i Stockholms, Malmöhus och Göteborgs- och Bohus län. De datorer som finns i storstadsområdena är i allmänhet större än de i övriga delar av landet. Med hänsyn härtill är den andel av databehandlingen som utförs i storstadsområdena ännu större än andelen där befintliga datorer.

DASK framhöll att det borde vara möjligt att även med den nuvarande datakraftstrukturen ta ökad hänsyn till krigs- och beredskapsaspekterna genom att geografiskt sprida datacentralerna i landet. Detta har även skett i viss utsträckning. Man borde även se till att dessa hade så kompatibla datorutrustningar att det under krigs- och beredskapsförhållanden på någon eller några platser fanns tillgång till reservkapacitet för sådan databehandling som var avsedd att fungera i krig.

Den från beredskapssynpunkt ogynnsamma lokaliseringen av datorer inom landet har beaktats av ÖEF vid utarbetandet av anvisningarna för planläggning av informationsbehandling i krig (Anv Infob K).

SÅRK konstaterar att den geografiska koncentrationen av datorer är en allvarlig sårbarhetsfaktor. Med en stor del av databehandlingen lokaliserad till storstadsområdena, främst Storstockholmsområdet, kan vid bombanfall och liknande intensiva angrepp en stor del av landets datorkraft slås ut tämligen omgående.

5.4 Integration och inbördes beroende

5.4.1 *Systemmässig samordning*

Den mest långtgående samordningen innebär att olika användare inom ramen för ett gemensamt system använder samma personal för utveck-

ling, underhåll och drift av ADB-system, samma datorer och annan ADB-utrustning samt helt eller delvis samma register/databaser och program. Sådan samordning brukar ibland kallas systemmässig samordning eller applikationssamordning och förutsättningen för en sådan kan bl a vara att samma data i stor utsträckning används i olika verksamheter, att i stort sett samma grupp individer (företag, fastighet etc) berörs eller att man har behov av ungefär samma typ av bearbetningar.

Långtgående systemmässig samordning har naturligtvis fördelar att erbjuda och kan bl a ge reducerade kostnader genom exempelvis minskat dubbelarbete. Detta är emellertid fördelaktigt endast till en viss gräns eftersom samtidigt komplexiteten och därmed också trögheten mot förändringar växer. Härigenom tenderar sårbarheten att växa. Långtgående systemmässig samordning kan enligt SÅRKs mening vara ett från sårbarhetssynpunkt mindre lämpligt alternativ.

En mindre långtgående form av samordning kan vara att göra gemensam systemutveckling och gemensamt systemunderhåll för ett antal likartade men separata system avsedda för olika tillämpningar. Detta kan leda till minskning av sårbarheten genom att man skapar ökade möjligheter att låta systemen tjäna som reserver för varandra.

En ännu mera begränsad samordning än de som nu beskrivits kan ske genom datautbyte mellan skilda system.

5.4.2 *System- och informationsberoende*

I fortsättningen skall i huvudsak behandlas samordning och beroende genom datautbyte.

Ett omfattande informationsflöde förekommer i dag mellan olika system. Hur omfattande detta flöde är har inte kartlagts i detalj. Vissa system används mer eller mindre som bas- eller uppdateringsregister för andra system. Vad gäller grunduppgifter om fysiska personer kan som exempel nämnas ADB-systemet för folkbokföring och beskattning, Datemas befolkningsregister och SPAR. Som exempel på basregister för företag och organisationer kan nämnas det hos SCB förda centrala företagsregistret (CFR) och RSVs organisationsnummerregister. Vad gäller fastigheter kan CFDs register och RSVs register för fastighetstaxering ges som exempel.

Härutöver sker ett omfattande informationsutbyte vad gäller bl a administrativa data mellan olika myndigheter, mellan myndigheter och företag och mellan företagen. Det kan gälla skatteuppgifter, betalningstransaktioner av olika slag, orderuppgifter mellan företagen osv.

En mängd olika uppgifter går från olika adminstrativa system till system för samhällsplanering och statistik. I det följande skall dataflödena i någon mån exemplifieras.

RFVs system byter en mängd uppgifter med andra system.En sammanställning inom verket gjord den 16 september 1977 över volymer transaktioner vid samkörning/avisering via magnetband visar bl a följande resultat

- Löpande aviseringar till RFV 45,6 milj transaktioner/år
- Löpande aviseringar från RFV 24,5 milj transaktioner/år

Bland mottagare och leverantörer kan nämnas
- bankgirocentralen
- postbanken
- postverket
- rättsväsendets informationssystem
- RSV
- kommuner
- länsstyrelser
- arbetsmarknadsstyrelsen
- centrala studiemedelsnämnden
- civilförsvarsstyrelsen
- försvarets civilförvaltning
- VPV
- bygghälsans forskningsstiftelse
- SCB
- statens personalpensionsverk
- SPADAB

I övrigt kan nämnas att centrala bilregistret (CBR) och centrala körkortsregistret (CKR) samt SPAR förser och kommer att förse en mängd externa system med information. CBR lämnar uppgifter till t ex försäkringsbolag, SCB, RPS och VPV bl a genom direktkommunikation via terminal. Mellan RPSs och TSVs anläggningar finns dator-datorförbindelse med vars hjälp ömsesidigt informationsutbyte sker. Det har även inrättats dator-datorförbindelse mellan vissa större försäkringsbolag och CBR.

Det är i och för sig tekniskt möjligt och därför inte osannolikt att framöver dator-datorförbindelser kan komma att upprättas mellan exempelvis SPAR och
- Försäkringsbolag
- UC och vidare till samtliga affärsbanker
- SPADAB och vidare till samtliga sparbanker
- ABAK/Justitia Kreditupplysningsföretag
- Kommun-Data
- Stockholms, Göteborgs och Malmö kommuner
- Lantbruksdata
- RPS
- Kronofogdemyndigheterna (REX)
- Arbetsmarknadsverket
- VPV
- CFD
- Centrala studiestödsnämnden (CSN)
- RSV och vidare till samtliga länsstyrelser
- Fackföreningar (LO-data, TCO etc)

Vidare kan sådan förbindelse tänkas upprättas mellan exempelvis CFD och

- Försäkringsbolag
- UC
- ABAK/Justitia
- Kommun-Data
- Stockholms, Göteborgs och Malmö kommuner
- Lantbruksdata
- SPAR
- RSV
- REX

I en förteckning upprättad den 8 september 1977 inom datainspektionen över stora statliga ADB-projekt som ännu inte fått sin slutliga utformning anges projektens knytningar till andra system. Av denna förteckning framgår bl a följande.

- I RSVs RS-projekt finns knytningar till RFVs register
- I RSVs REX-system finns knytningar till kreditupplysningsbranschen, RPS, länsstyrelsernas register, socialregister och skattekrediteringsregister
- CFDs koordinatsatta personband är aktuella för samkörning med SCBs folk- och bostadsräkningar, med SCBs lantbruksregister, med RSVs skatteband, med CKR, med vägverkets vägdatabank och med SCBs företagsregister
- I STUDOK-systemet (studiedokumentationssystem för högskolan) finns knytningar till SCB, AMS, CSN och RFV
- I miljövårdens informationssystem finns knytningar till SCB och arbetsmiljöregistren.

Ett omfattande flöde av data går mellan bankerna samt mellan bankerna och närliggande inrättningar som bankgirot, postgirot, UC, VPC osv. Bankgirot och postgirot har även utbyte på datamedium med bl a större företag och myndigheter. Behovet av åtkomst till data i andra system kommer att öka allt eftersom realtidsteknik med möjlighet till direktåtkomst till data med hjälp av terminaler blir vanligare i olika system. DASK framhåller att redan med dagens teknik och telekommunikationer kan systemoberoende åtkomst — med systemoberoende åtkomst menas möjligheter att från terminaler inte enbart hämta data i det egna systemet utan även från andra system samt att från särskilda terminaler hämta data från flera system — eller därmed jämförbar åtkomst av data i olika system rent tekniskt åstadkommas på flera olika sätt, t ex med hjälp av särskilda kommunikationsdatorer och dator-datorförbindelser.

Systemoberoende åtkomst kommer emellertid även att innebära ett ökat systemberoende i den meningen att olika system för att kunna kommunicera med varandra måste tillämpa samma procedurer och standarder i en rad avseenden. Det kan gälla gemensamma standarder i fråga om terminaler och programvaror. Vidare kan det gälla innehållsmässig och utseendemässig enhetlighet beträffande registerinne-

håll. I den mån det rör sig om automatiska aviseringar av olika slag genom terminal eller dator-datorförbindelse ökar detta systemberoende. I utvecklingens förlängning närmar man sig i vissa avseenden den systemmässiga samordning som beskrivs i avsnittets inledning. Det kan i detta sammanhang nämnas att det allmänna datanätet möjliggör fri uppkoppling mellan olika terminaler och datacentraler vilket givetvis ökar möjligheterna till integration.

Sammanfattningsvis kan sägas att det redan idag förekommer ett avsevärt beroende mellan olika system. Den framtida tekniska utvecklingen främst på kommunikationssidan kan komma att öka detta beroende. Från sårbarhetssynpunkt innebär detta att skador, störningar eller felaktigheter i ett system får negativa återverkningar i andra system.

5.5 Bearbetningsmöjligheter vid ansamling av stora datamängder

5.5.1 *Stora datamängder*

Användning av ADB gör det möjligt att sammanföra och överblicka mycket stora kvantiteter information. När det gäller personuppgifter kan man samla information om ett stort antal människor och sammanföra ett mycket stort antal uppgifter om varje person. Flera stora system med personuppgifter finns idag uppbyggda såväl inom den privata som offentliga sektorn. En myndighet som förfogar över stora datamängder är SCB. Hos SCB finns ett stort antal personregister och andra register av varierande bredd och djup. SCB håller även på att utveckla ett arkivstatistiskt system ARKSY. Inom detta byggs bl a upp en regionalstatistisk databas (RSDB) och en företagsdatabas. SCB bygger en stor del av sin statistikproduktion på material som samlas in av andra myndigheter för primärt annat syfte än statistik. Vidare samlar SCB in uppgifter från företag och allmänhet genom postenkäter och genom telefon- eller besöksintervjuer. Några av SCBs register skall nämnas.

Folk- och bostadsräkningar genomförs sedan 1960 med hjälp av ADB. Dessa register innehåller uppgifter om samtliga invånare i Sverige. Registret över totalbefolkningen (RTB) är ett annat register som innehåller hela befolkningen. Inkomst- och förmögenhetsregistret innehåller uppgifter om större delen av befolkningen. Bland de känsligare registren kan nämnas olika register för brottsstatistik och socialhjälpsstatistik. Sammanlagt har SCB över 100 personregister. Dessutom finns en mängd andra register som inte är personorienterade, t ex olika företagsregister.

System för samhällsplanering innehåller i regel både djup och bred information av olika slag.

Även hos RFV finns stora datamängder i ADB-systemet för den allmänna försäkringen m m. Andra exempel på register med stora datamängder är bil- och körkortsregistret, UCs kreditupplysningsregister samt register hos större banker och försäkringsbolag.

Stora datamängder samlas även på samma ställen genom att vissa servicebyråer har en mängd kunder. Det stora flertalet kommuner anlitar Kommundata AB. Härigenom samlas mängder av data från landets kommuner hos detta servicebolag. På samma sätt fungerar DAFA och universitetens datamaskincentraler inom den statliga sektorn. Även på den privata sidan finns servicebyråer med ett stort antal kunder.

Ytterligare några register som inte i första hand är personorienterade skall nämnas. Inom det tidigare nämnda miljövårdens informationssystem (MI) finns en del sådana. Syftet med MI är att successivt bygga upp en informationscentral för den information på miljöområdet som bl a myndigheter behöver för sitt arbete.

Som tidigare framhållits innehåller CFDs register uppgifter om alla fastigheter i landet och vägdatabanken information om vägar, broar m m.

5.5.2 *Bearbetningsmöjligheter, användning för annat syfte än det ursprungliga*

Med hjälp av ADB kan man alltså lagra stora informationsmängder. Den största vinsten med datorer som hjälpmedel vid administrativ och teknisk-vetenskaplig databehandling ligger emellertid i möjligheten att snabbt bearbeta och ta fram önskad information. Bearbetning kan ske genom sortering, sammanställning av olika uppgifter, jämförelse av en uppgift med annan, urval av vissa uppgifter etc. De möjligheter som automatisk databehandling medför är i detta sammanhang av särskild betydelse. Som påpekas av offentlighets- och sekretesslagstiftningskommittén i betänkandet Data och integritet (SOU 1972:47) har underrättelseverksamhet sedan gammalt i mycket stor utsträckning bedrivits genom sammanställning av ett stort antal i och för sig banala och ofta offentligt tillgängliga uppgifter varigenom slutsatser kunnat dras i frågor omgivna av militär och kommersiell sekretess.

Enligt betänkandet Den militära underrättelsetjänsten (SOU 1976:19) används redan nu datorer i viss utsträckning vid bearbetning av underrättelser vid försvarsstabens underrättelseavdelning. I betänkandet sägs att en ökad effektivitet vid bearbetningen torde kunna åstadkommas om datatekniken tas i anspråk ännu mer vid registrering, lagring och övrig behandling av underrättelsematerialet.

Att datorer används även av andra länders underrättelsetjänst står helt klart. I den mån man i sådan verksamhet kan komma över uppgifter som redan finns lagrade på datamedium underlättar detta naturligtvis arbetet.

Möjligheterna att samla, lagra och bearbeta information med hjälp av ADB har gett förutsättningar att höja servicegraden inom många sektorer av vårt samhälle. Fördelarna med ADB-användning kan emellertid som ovan nämnts även utnyttjas för ändamål som på olika sätt kan vara skadliga för vårt land, t ex genom att information av olika slag sammanställs för att användas i andra länders underrättelsetjänst. Detta är ett

exempel på hur information används på ett sätt som är helt annat än det ursprungliga. Ett annat exempel är att känslig information används för utpressning för bl a politiska syften. I en krigssituation kan register som tillkommit för administrativa-statistiska eller samhällsplaneringsändamål användas av främmande makt som hjälpmedel att kontrollera landets innevånare och som hjälpmedel att få fram olika nyckelpersoner etc. Vid planläggning av och vid ett eventuellt genomförande av angrepp mot vårt land kan en främmande makt ha stor nytta av olika uppgifter som finns lagrade i dataregister. Exempel på sådana uppgifter är fakta om geografiska förhållanden (vägar, järnvägar, broar m m), om vår produktionsapparat (kapacitet och lokalisering) och om vår kraftförsörjning.

5.6 Bristfällig kunskap hos datoranvändare m m

5.6.1 *Bristfällig utbildning och kunskap som sårbarhetsfaktor*

Av de myndigheter och företag som SÅRK intervjuat svarade de flesta att de inte funnit bristfälliga kunskaper hos användarna som någon påtaglig sårbarhetsfaktor. Några av de intervjuade nämnde dock att denna faktor medfört vissa initialproblem i samband med att nya system skulle köras igång. En av de tillfrågade framhöll att ett intensivt utbildningsarbete bedrevs innan man vågade ta ett nytt omfattande system i drift. Ytterligare en menade att det många gånger var svårt att få korrekta indata på grund av att personalen inte läste instruktionerna. Vad gäller oavsiktliga misstag såg de intervjuade dock inte heller detta som någon påtaglig sårbarhetsfaktor. Det var snarare frågan om ett irritationsmoment som ibland kunde få vissa ekonomiska konsekvenser. En av de tillfrågade framhöll att misstag på grund av okunnighet hos terminalanvändare kunde förorsaka besvärande avbrott i hela system.

Även om många av de intervjuade inte funnit kunskapsnivån hos användarna som någon påtaglig sårbarhetsfaktor kan man inte bortse från betydelsen av utbildning på olika nivåer när man diskuterar sårbarhetsfrågor.

Rent allmänt kan sägas att goda kunskaper hos såväl konstruktörer som användare av olika slag är en förutsättning för väl fungerande och säkra datasystem. Exempelvis blir ett system som från början eller genom ett antal ändringar fått en onödigt komplicerad och oöverskådlig uppbyggnad mer sårbart för angrepp utifrån. Det kan bli svårare att hindra eller att upptäcka manipulationer av olika slag i ett sådant system.

Av de rena dataspecialisterna som systemerare, programmerare och operatörer måste krävas goda kunskaper om såväl hårdvara som mjukvara. Den nära samverkan mellan program- och maskinvara i ett datorsystem kräver allsidiga tekniska kunskaper av dem som skall bygga upp ett väl fungerande ADB-system. Det gäller att välja rätt programvara och använda den på rätt sätt. Teknikern måste även kunna lösa olika säker-

hetsproblem. Det kan t ex gälla att skydda känslig information genom att olika spärrar och behörighetskoder byggs in i systemet. Brister i systemvaran behandlas i ett senare avsnitt. Olika beslutsfattare som är ansvariga för anskaffning av datorsystem behöver även kunskaper för att kunna välja ett system lämpat för den verksamhet det är avsett för. Risk finns, då ett system fungerar dåligt, att det krävs diverse improvisationer som kan öka sårbarheten. Det gäller även att redan från början ha klart för sig vilken säkerhetsnivå som krävs.

Även de rena användarna, alltså de som skall utnyttja den information som ett ADB-system lämnar eller de som lämnar uppgifter till systemet, behöver utbilding. Värdet av ett tekniskt fulländat system minskar om inte användarna vet vilka möjligheter och begränsningar systemet har och hur det rent tekniskt skall användas. I en revisionspromemoria upprättad den den 1 mars 1977 av Svenska Kommunförbundet rörande en kommuns datacentral heter det vad gäller utbildning bl a följande.

Utbildning på användarsidan är inte genomförd och utbildningsplaner saknas. — Verksamheten vid datorcentralen bör bedrivas på ett sådant sätt att garantier skapas för en effektiv och korrekt produktion. En förutsättning för att uppnå detta tillstånd är att datoranvändarna bibringas erforderlig information och kunskap. Då verksamheten i kommunen i huvudsak drivs i egen regi, med egen datacentral, och då datarutinerna är speciellt utformade för kommunen är det ytterst angeläget att resurser satsas på utbildning av dataanvändarna och att utbildningen är direkt anpassad till användarnas arbetsuppgifter. — Enligt vad vi erfarit har ytterst små insatser gjorts för att bibringa dataanvändarna erforderliga kunskaper. En grundläggande kurs i ADB-orientering har genomförts. Däremot har inte planerats för en utbildning som är direkt styrd mot användarnas arbetsuppgifter. Vi finner det vara ytterst angeläget att åtgärder vidtas för att korrigera bristen.

Det kan i detta sammanhang nämnas att enligt olika undersökningar är oavsiktliga fel och underlåtenheter det största hotet mot ADB-säkerheten. I statskontorets rapport 1975:9 Dataskydd drogs bl a följande slutsatser från en studie som omfattade nio datacentraler på den offentliga och privata sektorn.

De flesta hoten[1] uppträder därför att enkla rutiner inte fungerar som väntat. Hoten kan också vara väl kända hos den operativa personalen vid en anläggning dvs hos de personer som sköter den dagliga produktionen. Personalen accepterar hotens förekomst, antingen för att den inte känner riskerna eller för att eventuella åtgärder är obekväma eller tidsödande att utföra. Cheferna är ofta inte medvetna om hotens existens och vidtar följaktligen inte heller några åtgärder. — Många hot gäller kommunikationsproblem mellan olika befattningshavare. Information av olika slag missuppfattas lätt, vilket leder till felaktiga åtgärder. — De iakttagna hoten tyder också ofta på svagheter i samverkan mellan personal och maskinell utrustning. Beslut skall fattas av olika befattningshavare, som skall överföra instruktioner till maskinerna via manöverbord, knappar, inställningsrattar, indata etc. Maskinutrustningen, exempelvis datorer, minnesenheter, skrivare och efterbehandlingsmaskiner, svarar med att utföra beordrade instruktioner och begär eventuellt att en ny åtgärd skall vidtas. Under denna kommunikationsprocess kan missförstånd och felaktiga handgrepp förekomma.

[1] Med not avses i rapporten en störning som skulle kunna inträffa

Ett av skälen till oavsiktliga fel är naturligtvis bristfälliga rutiner men beror säkert ofta också på bristande kunskaper hos användare. För att underlätta operatörernas arbete och minska riskerna för felgrepp bör säkra rutiner skapas och olika rimlighetskontroller byggas in i systemen.

Bristande kunskaper inom ADB-säkerhet kan i hög grad bidra till att öka sårbarheten i olika ADB-system. SÅRK instämmer i vad som inledningsvis sägs i IBMs datasäkerhetshandbok, anvisningar för utbildning i datasäkerhet.

Ett datasäkerhetssystem kommer aldrig att fungera om inte berörd personal utbildas i datasäkerhet. — Den personal som berörs finns ofta på flera avdelningar och är ofta fler till antalet än man till en början tror. Olika typer av utbildning måste ges eftersom behoven varierar. Utbildningen skall ges under lång tid och samordnas med övriga aktiviteter i datasäkerhetsarbetet. — På sikt bör utbildningen i datasäkerhetsfrågor ges i all utbildning i ADB och i allmän säkerhet. Datasäkerhetsproblemen kan då sättas in i sitt rätta sammanhang. I avvaktan på detta måste utbildning i datasäkerhet även ges fristående. — Förutsättningarna för att utbildningen i datasäkerhet liksom all annan utbildning skall lyckas är att den ges tidigt, samordnas med andra parallella aktiviteter och följs upp med återkommande utbildningstillfällen. Utbildningen är inte bara en del av datasäkerhetsarbetet, den fungerar också som en drivkraft. — Det är ingen överdrift att säga att utan tidig utbildning — ingen datasäkerhet.

5.6.2 *Något om utbildningsläget*

I dataindustriutredningens betänkande Data och Näringspolitik 74 (SOU 1974:10) sades att utbildning i datatekniska ämnen huvudsakligen bedrivs av följande institutioner och företag

- utbildningsväsendet
- studie- och folkbildningsförbund
- specialiserade tjänsteföretag
- leverantörer av datasystem
- intresse- och branschorganisationer, samt övriga användargrupperingar (större företag m fl)

Vad gäller den allmänna och grundläggande ADB-utbildningen inom utbildningsväsendet konstaterade dataindustriutredningen att ingen organiserad undervisning om databehandling bedrivits i grundskolan under läsåret 1972/73 medan vissa aktiviteter förekom på gymnasienivå.

Dataindustriutredningen framhöll

- att förstärka ADB-utbildningsåtgärder var den mest betydelsefulla näringspolitiska åtgärden på data området
- att utbildningsåtgärderna i första hand borde inriktas mot en förstärkning av användarkompetensen i landet
- att utbildningen av specialister härigenom fick en vidgad rekryteringsbas för intensifierade åtgärder för systemkonstruktörsutbildning på olika nivåer.

Dataindustriutredningen torde ha utgjort en av de pådrivande krafterna för att vidga ADB-utbildningen. Sedan 1974 pågår inom skolöverstyrel-

sen (SÖ) det s k DIS-projektet (Datorn I Skolan). Arbetet går bl a ut på att ge en allmänutbildning om datorer och datorers användning. Försöksverksamhet i större skala inleddes läsåret 1976/77. En rapport från första årets verksamhet har lagts fram i januari 1977. Tanken är att datalära skall ingå i ämnena matematik och samhällskunskap i såväl grundskola, gymnasieskola som i kommunal vuxenutbildning. Vidare bedrivs försöksverksamhet med datoranvändning i vissa bygg- och eltekniska ämnen på fyraårig teknisk linje.

Inom LO och TCO tillsattes under 1976 arbetsgrupper vilka har framhållit vikten av utvidgad datautbildning.

Det kan även nämnas att Riksdataförbundets medlemmar verkat för en förbättrad utbildning inom olika ADB-områden bl a vad gäller datasäkerhet. Vidare ges kurser i datasäkerhet av bl a statens institut för personaladministration och personalutbildning (SIPU) och av näringslivets säkerhetsdelegation.

Vad gäller universitets- och högskoleutbildning förekommer ADB-utbildning av varierande slag inom olika fakulteter och på de tekniska högskolorna. Bl a kan nämnas att tekniska högskolan i Linköping 1975 startade en ny civilingenjörsutbildning som täcker både maskin- och programvara.

5.6.3 *Sammanfattande synpunkter*

Som framkommit har behovet av utbildning i datafrågor tillmätts allt större betydelse under senare år. Detta gäller såväl utbildning av mera allmän karaktär som utbildning av specialister. Särskilt kan noteras det ökade intresset för datasäkerhet och utbildningsfrågor i samband härmed. Om man först ser på SÖs arbete med att förbättra undervisningen i grund- och gymnasieskolan föreligger detta arbete fortfarande i stort sett på försöksstadiet. Det torde dröja ännu ett antal år innan undervisningen i datalära kommer att bedrivas allmänt inom landets skolor. Man får då även beakta att det kan ta rätt lång tid att utbilda ett tillräckligt antal lärare. Vidare är det fråga om resurser vad gäller datorutrustning etc. En omfattande utbildning sker dock inom andra institutioner och företag. Framförallt sker en omfattande internutbildning hos användarna.

Sammanfattningsvis kan följande sägas

- att det är värdefullt om grundutbildning införs som leder till baskunskaper som kan ligga till grund för vidareutbildning av olika kategorier som berörs av ADB-verksamhet
- att det i avvaktan på att denna grundutbildning kan komma att genomföras är viktigt att en omfattande utbildningsverksamhet drivs av användarföretag, organisationer, studieförbund etc
- att det i utbildningen av tekniker och systemerare även läggs stor vikt vid säkerhets- och sårbarhetsfrågor
- att man bör se till att olika yrkeskategorier som kan komma att få inflytande över anskaffning av datorsystem får en allsidig utbildning

inom ADB-området där vikt läggs även på säkerhets- och sårbarhetsfrågor
- att det är betydelsefullt att användare får lämplig utbildning för att klara av det dagliga arbetet.

5.7 Bristande kvalitet i fråga om maskin- och programvara

I fråga om driftsäkerheten kan som tidigare framhållits maskinvaruutrustningen numera anses ha hög tillförlitlighet. Däremot kan programvaran utgöra ett problem. Detta gäller inte minst operativsystemen i stora datorer för avancerad databehandling.

I Ingenjörsvetenskapsakademiens rapport Framsteg inom forskning och teknik 1973 beskrivs i ett avsnitt datorutvecklingen och datortillämpning. I detta avsnitt berättas bl a om leverans av en superdator, ILLIAC IV till en NASA-institution i Kalifornien under år 1972. Superdatorn, som i själva verket var uppbyggd av 64 individuella datorer togs som utgångspunkt för att beskriva problem med maskinvara och programvara. Det som beskrevs ligger visserligen några år tillbaka i tiden men visar ändå på problem som ännu inte är lösta. Bl a sägs följande.

Superdatorernas intåg ställer ett problem, som länge varit besvärande, i blixtbelysning. Alla de 64 processorerna var väl uttestade när de levererades, men att bygga ihop ILLIAC IV med alla dess perifera enheter och stöddatorer har redan tagit två år, och är inte alls ett avslutat kapitel. Det är här inte bara fråga om att få maskinvaran att fungera som en enhet. — Alla de programvarusystem som skall fogas ihop kan beräknas innehålla olika typer av fel och inkonsekvenser i relationerna till varandra. Erfarenheterna har visat att i stora programsystem når man aldrig felfrihet, utan möjligen en konstant låg nivå av fel, som successivt upptäcks, rättas till och ersätts av andra fel. Programvaran modifieras ju efter hand, och man kan aldrig räkna med att de nya moduler som förs till är felfria eller på ett perfekt sätt samspelar med det som sparas från tidigare versioner — där som sagt okända avvikelser från tänkt funktionssätt också finns och på ett sätt gör det logiskt omöjligt att konstruera en perfekt ny modul för inkoppling. — Frågan hur maskin- och programvara skall byggas upp för att detta problem skall hållas under kontroll har sysselsatt forskarna alltsedan datorernas första år. Nyligen har intresset stegrats, både på grund av att de allt större systemen för administrativ databehandling, där smärre fel ej ger katastrofala effekter, måste göras driftsäkrare för att bli accepterade och ekonomiskt konkurrenskraftiga, och på grund av att system för styrning av exempelvis järnvägstrafik helt enkelt måste göra varje beslut korrekt, för att inte förorsaka kollisioner eller urspårningar. — Tekniken för att göra datorerna säkrare har sammanfattats under benämningen Fault-Tolerant Computing. Redan ämnesområdets benämning antyder, att man inte kan räkna med att annat än mycket enkla datorsystem kan garanteras vara alldeles rätt programmerade, och att man under alla förhållanden måste räkna med att komponenter i datorn går sönder, störs av yttre signaler etc, och därigenom ger permanenta eller tillfälliga felaktiga beräkningsresultat i något led. — Fault-Tolerant Computing innebär, vad avser maskinvaran, att man bygger in tillräcklig säkerhet i denna för att upptäcka tillfälliga och permanenta hårdvarufel och i möjligaste mån korrigera dessa (via redundanta koder m m). Man får härvid

använda olika filosofi med hänsyn till vad konsekvenserna av ett oupptäckt fel, som resulterar i att systemet ger felaktiga utdata, kan bli, respektive vilka åtgärder man önskar vidtaga omedelbart eller efter viss tid med hänsyn till ett upptäckt fel. — Metoderna att hantera säkerhetsfrågorna för programvaran är ännu ej lika väl utvecklade, och här återstår arbete på många fronter.

I konferensdokumentation från Nord-Data 1977[1] beskrivs ett forskningsprojekt om programvarukvalitet. Problemet, dess orsaker och förslag till åtgärder framställs på följande sätt.

I initierade kretsar har man sedan flera år tillbaka talat om programvarukrisen. Med denna har man avsett de snabbt växande problemen vid framställning av programvara. Den snabbt ökande storleken, komplexiteten och betydelsen av programvara har medfört att leveransförseningar, kostnadsökningar och låg produktkvalitet blivit mycket vanliga i branschen. — Det finns flera orsaker till dessa problem. Det saknas ett samlat kvalitetsmedvetande hos såväl producenter som kunder. Detta beror delvis på dålig utbildning, men framförallt på att det saknas allmänna metoder för specifikation och bedömning av kvalitet hos programvara. De egenskaper hos program som går att möta — t ex minnesutnyttjande — har därför kommit att överbetonas. Intresset har också koncentrerats kring framtagnings- och körkostnader snarare än livstidskostnader och indirekta kostnader. Detta har ytterligare ökat skevheten i bedömningen av programvara. — Branschen har dessutom avsevärda organisations- och metodikproblem. Framtagning av programvara utfördes ursprungligen som enmansprojekt, och nästan alla metoder och hjälpmedel har utvecklats för fåmansprojekt. Från detta utgångsläge har projekten sedan växt utan att erfarenheter från andra branscher utnyttjats. Tekniken har kommit att överbetonas och de organisatoriska aspekterna att försummas. — För att situationen skall kunna förbättras krävs att det utvecklas metoder för att möjliggöra styrning av produktion av programvara mot en för varje produkt optimal kvalitet. Sådan kvalitetsstyrning förekommer idag inte i programvarubranschen men är vanlig inom andra branscher. För att detta skall vara möjligt behövs metoder för att specificera och kontrollera kvaliteten. Detta behöver inte enbart innebära mätmetoder. Krav på ändringsbarhet hos program kan t ex uppfyllas genom en starkt moduliserad konstruktion, men kan knappast mätas direkt på produkten. Därför är det viktigt att också själva framtagningsprocessen kan dokumenteras. — Det är också mycket viktigt att metoder för kvalitetsstyrning och dokumentation och specifikation av kvalitet verkligen sprids till producenter och kunder. En nödvändig åtgärd är därför sammanställning av praktiskt användbara handböcker och kurser i kvalitetsstyrning. — Liksom i andra branscher kan det även i programvarubranschen bli aktuellt med samhällskrav på kvaliteten hos programvara. Sådana krav kan t ex vara en längsta tid för spärrning eller rättning av felaktig information i en allmänt tillgänglig databas.

I en amerikansk senatsrapport[2] beskrivs några fall där fel i programmen vållat i vart fall stora ekonomiska förluster. Ett system som användes av den amerikanska armén för att planera transporter av material till kunder på andra sidan haven visade sig felprogrammerat. Detta medförde att material hämtades från fel förråd, något som föranledde onödiga transportkostnader med 900 000 dollar om året. Dessutom ådrog man sig 1,3 miljoner dollar i ökade investeringskostnader.

Ett system använt som hjälpmedel av amerikanska flottan för att planera översyn av komponenter möjliga att reparera för framtida an-

[1] Programvarukvalitet — ett NORDFORSK-projekt, Anders Beckman och Jan Törnqvist

[2] Problems Associated With Computer Technology In Federal Programs And Private Industry, Computer Abuses, Washington 1976

vändning visade sig vara felprogrammerat. Resultatet blev miljontals dollar i onödiga kostnader på grund av obehövliga eller för tidigt gjorda översynsarbeten.

Vid SÅRKs intervjuer har framkommit att hos flera av de tillfrågade förekom fel i operativsystemen. Vissa av de tillfrågade nämnde att man haft besvär med applikationsprogram beroende på att utvecklingstiden varit för kort vilket omöjliggjort ordentliga tester av programmen. Hos en servicebyrå hade fel i programvaran medfört att en kund fått fram en annan kunds information. Två av de tillfrågade tyckte att det i on-line system var alltför lätt för obehöriga att få access till registerinformationen. I ett fall nämndes att man konstruerat ett eget program därför att standardvara inte fanns. Programmet blev mycket komplicerat och det tog ett år att få det i drift. Endast några få kan programmet och man är mycket beroende av att det fungerar. Maskinvarufel nämndes i två fall. I ena fallet kostade det en halv miljon kronor att rätta till felet.

Som framgått förekommer brister i såväl maskinvaran som programvaran. Även om fel i maskinvaran fortfarande är vanliga är sådana fel lättare att komma till rätta med än fel i programvaran. Ju större och mer komplicerade system desto större är risken att det kan finnas brister i programvaran. Framförallt medför ändringar i programmen följder som inte alltid kan överblickas. Ofta saknas tid att genomföra ordentliga tester. Ibland ligger felet inte i programvaran utan i att man använder den felaktigt eller på ett sätt som den inte varit avsedd för.

En möjlighet att minska riskerna för fel i programvaran ligger i en långt gående modularisering som underlättar ändringar och upptäckt av fel i den.

Fel och brister i maskin- och programvara förefaller inte vara någon allvarlig sårbarhetsfaktor utan snarast en källa till extra kostnader och förseningar. I många fall måste man dock ställa mycket höga krav på att systemen fungerar korrekt t ex vid trafikstyrning där fel kan leda till allvarliga olyckshändelser. Fel i programmen som inte upptäcks på en gång kan ge skador som sedan är omöjliga att reparera vilket i sin tur kan få allvarliga konsekvenser vad gäller viktiga och känsliga system.

5.8 Nyckelpersoner för datordriften

5.8.1 *Inledning*

Även om det brukar hävdas att ingen är oumbärlig torde det dock stå klart att vissa funktionärer är svårare att ersätta än andra. För specialister av olika slag, bl a inom dataområdet, kan det vara svårt att finna ersättare, i vart fall inom rimlig tid. Inom just dataområdet ställs krav på kunskaper om en komplicerad teknik men dessutom om hur denna teknik specifikt används inom ett vissa företag, hos en viss myndighet eller viss organisation. Många företag, myndigheter och organisationer har blivit helt beroende av att datordriften fungerar. Detta har medfört

att verksamheten även inom mycket stora företag och organisationer vilar på relativt få människor.

Beroendet av personer med nyckelposition för datordriften är naturligtvis en faktor av stora betydelse när man diskuterar sårbarhetsfrågor.

Systemerare och programmerare kan bygga upp komplicerade system, som ingen annan än de själva behärskar. Saknas dokumentation eller är dokumentationen bristfällig är då användaren helt i händerna på systembyggaren. Detta kan få menliga följder vid t ex sjukdom, olycksfall eller dödsfall. Även osämja mellan personal och uppdragsgivaren kan leda till sådana åtgärder från de anställdas sida att systemet görs obrukbart. Även personer inom den dagliga driften kan vara svåra att undvara eller ersätta.

5.8.2 *Missnöjda, ohederliga eller opålitliga medarbetare*

Det är allmänt bekant att skadeverkningar inom ADB-verksamhet förorsakade av missnöjda, ohederliga eller opålitliga medarbetare förekommer. Det föreligger emellertid en strävan att tysta ner händelser av denna art. Följande fall relateras i Kerstin Anérs bok Datamakt. En programmerare var anställd i ett företag som gick dåligt. Han hade blivit osams med sina chefer och antog att han själv snart skulle höra till dem som avskedades. Han programmerade företagets dator så att när uppgiften om hans eget avskedande matades in utplånade datorn informationen i sitt eget minne. Back-up i form av kopior saknades.

I boken Where Next for Computer Security (1974, theNational Computing Centre Ltd) finns ett liknande exempel. En magnetbandsbibliotekarie som blivit uppsagd passade under uppsägningstiden på att förstöra informationen på alla magnetband. Detta medförde förluster av data till ett värde av ungefär 10 miljoner dollar.

I Donn B. Parkers bok, Crime by computer, beskrivs hur en student lyckades skaffa sig kontroll över ett universitets hela time-sharing system. Studenten hade gjort ett användarprogram som han sedan skänkte till universitetet. I programmet hade han lagt in vissa specialinstruktioner som gjorde att när användarprogrammet för första gången brukades för körning på högsta behörighetsnivå — vilket skedde efter sex månader — så öppnades hela systemet för studenten. Det hela upptäcktes av en slump innan någon skada hade skett.

Man kan tänka sig många andra typer av angrepp som kommer inifrån, allt ifrån att programmerare manipulerar programmen så att informationsinnehållet förvanskas till att det förstörs eller att maskinutrustningen skadas. Som ytterligare exempel kan nämnas försäljning eller annat olovligt förfogande av information. Allvarliga följder skulle uppstå om olika politiska grupper började med infiltration bland anställda på datacentraler i syfte att förstöra eller manipulera datasystem.

Idag sker personalkontroll på den statliga sidan enligt personalkontrollkungörelsen (1969:446). Med personalkontroll förstås enligt kungörelsen att man inhämtar upplysningar ur polisregister om den som innehar eller avses tillträda tjänst som är av betydelse för rikets säkerhet.

Vilka myndigheter som får företa personalkontroll räknas upp i författningen. Dit hör t ex DAFA, SCB, RFV och televerket. Även några andra affärsdrivande verk och statliga bolag finns med i uppräkningen. Ytterligare myndigheter utöver de som räknas upp kan efter särskild framställning till regeringen medges rätt till personalkontroll. Personalkontroll får endast göras beträffande tjänst som är skyddsklassad. Två skyddsklasser finns, skyddsklass 1 och 2. Till skyddsklass 1 hör tjänster som är av synnerlig betydelse för rikets säkerhet och till skyddsklass 2 hör övriga tjänster av betydelse för rikets säkerhet. Framställning om utlämning av uppgifter för personalkontroll görs hos RPS som under medverkan av lekmannarepresentanterna i styrelsen avgör vilken information som skall lämnas ut. Myndigheten fattar sedan själv beslut huruvida en person skall anses olämplig för tjänsten eller ej. För den privata och kommunala sidan finns inte någon liknande författningsreglering om personalkontroll. Givetvis kan varje arbetsgivare i samband med anställning göra de kontroller och efterforskningar han anser erforderliga. I regel har dock inte en arbetsgivare rätt att ta del av information ur olika register som t ex kriminal- och polisregister.

De flesta intervjuade företag och myndigheter vidtog inte någon speciell kontroll avseende ADB-personal. En av de tillfrågade ansåg dock att det vore värdefullt om man ålades sådan kontroll. I två fall skedde vissa kontroller av ADB-personal. I ett av fallen ansåg sig företaget skyldigt till detta på grund av upphandling med staten.

Det kan nämnas att personal som skall anställas inom SWIFT-systemet utsätts för en ingående kontroll innan de anställs.

Vad gäller svenska förhållanden kan sammanfattningsvis sägas att någon personalkontroll av ADB-personal inte sker i någon större omfattning. Det kan dock konstateras att vill man infiltrera ett system i syfte att skada detta på något sätt finns det, visar all erfarenhet från andra likartade situationer, alltid villiga personer tillgängliga som utåt verkar helt oförvitliga. Personalkontrollen kan av många skäl inte göras till ett fullständigt effektivt instrument.

Ett annat sätt att minska riskerna för olika manipulationer inifrån är att göra flera personer beroende av varandra t ex för att få tillgång till viss information eller för att kunna utföra olika körningar.

5.8.3 *Förhållanden vid beredskap och krig m m*

Beroendet av personer med nyckelposter får även stor betydelse vid beredskaps- och krigssituationer. Bl a får man räkna med att flera personer som är viktiga för datordriften såväl på den offentliga som den privata sektorn blir inkallade. I ÖEFs anvisningar för planläggning av informationsbehandling i krig vad gäller statliga myndigheter heter det bl a

> ADB-personal är i betydande omfattning krigsplacerad i befäls- eller specialistbefattningar inom krigsmakten. Detta medför stora problem vid omfattande inkallelser. Vissa kategorier som systemprogrammerare och operatörer är också

svåra att ersätta med annan personal. Nyutbildning av dessa kategorier i ett krigsläge är inte realistiskt med hänsyn till den långa utbildningstid som krävs. Den personalkategori som går snabbast att utbilda är stanspersonal. Eftersom informationsbehandlingsbehovet i de flesta fall blir mindre i krigstid, samtidigt som personalen endast skall användas för drift och underhåll av krigsnödvändiga informationssystem, blir behovet av ADB-personal mindre än i fredstid. — Välutbildad personal liksom god driftdokumentation underlättar möjligheterna till omplaceringar. En långt driven fredstida specialisering kan däremot försvåra en omställning i ett krigsläge.

Motsvarande torde gälla även på den kommunala och privata sektorn. Visserligen finns uppskovsmöjligheter men dessa är inte alltid så stora. Enligt en utredning som gjorts av AMS och SAF utgörs ADB-personal till 80 % av värnpliktiga i befäls- och specialistfunktioner, något som medför att de militära myndigheterna inte vill avvara dem. Med en jämnare könsfördelning över hela ADB-området skulle konkurrensen mellan försvarsmakten och den civila sidan inte blir ett lika stort problem.

Inför en krigssituation kan just datapersonal vid viktigare datacentraler höra till de nyckelpersoner i samhället som en eventuell fiende skulle kunna tänkas vilja oskadliggöra. Sådana personer kan även vara intressanta objekt för angrepp från olika terroristorganisationer. Att hindra personal från att utöva sina funktioner inom datordrift kan vara ett effektivt sätt att sabotera verksamheten.

5.8.4 *Konflikter på arbetsmarknaden m m*

Vid konflikter på arbetsmarknaden kan strejkvapnet användas så att nyckelpersoner inom olika områden tas ur produktionen. Genom att så många är beroende av att datordriften fungerar kan stora effekter åstadkommas genom att enbart personal inom dataområdet tas ut i strejk. Det kan t ex gälla programmerare, operatörer men även personal som står för datorernas service som t ex reparatörer. Det kan vara driftkontrollgrupper etc. I den mån andra system är beroende av det som direkt berörs av konflikten ökar effekten ytterligare.

Av de myndigheter och företag som tillfrågats hade ingen någon egentlig planering inför en strejksituation. I något fall hade man börjat överväga vissa manuella rutiner. En av de tillfrågade upplyste att, om strejken skulle gälla systemerare, skulle man förbjuda ändringar i programmen för att på det sättet få säkrare drift. De flesta svarade att det inte gick att göra så mycket vid en strejk utan att det blev fråga om strejkbryteri. Andra menade att särskild planering var obehövlig eftersom arbetsgivarsidan omedelbart skulle komma att svara med omfattande lockout eller stor-lockout.

Någon allvarlig konflikt inom ADB-området har ännu inte inträffat i vårt land. Hösten 1977 inträffade emellertid en kortare strejk som rörde försäkringsbranschens datapersonal. Strejken varade tio dagar. Trots att strejken varade så pass kort tid och de strejkande inte föreföll särskilt motiverade samt att företagets möjligheter att förbereda sig inför strej-

ken var goda visade det sig att ett av försäkringsbolagen hade återstartsproblem som var långt ifrån obetydliga.

Det finns skäl att anta att mera omfattande konflikter av liknande slag kan medföra avsevärda störningar i samhällsmaskineriet.

Avslutningsvis skall nämnas något om intervjusvaren på frågan om verkningarna av att personer som sitter i nyckelställning inom ADB-verksamheten inte längre finns kvar i sina befattningar. De allra flesta skulle klara ett bortfall av två medarbetare. Ett bortfall av sex medarbetare ansågs i vissa fall medföra betydande svårigheter i form av driftstopp. När man kom upp till tolv personer ansåg de flesta att det kunde bli allvarliga svårigheter eller rent av totalstopp i hela datordriften. Endast några intervjuade menade att man skulle klara sig något så när oskadd vid ett sådant bortfall. Flera framhöll att det framförallt var på utvecklingssidan som det skulle bli bekymmersamt. Det bör påpekas att de intervjuade företagen och myndigheterna tillhör de största med stora datacentraler med ett stort antal anställda.

5.9 Dokumentation

SÅRK har vid de företagna intervjuerna uppmärksammat frågan om dokumentationens betydelse för sårbarheten.

Intervjuerna visar att man tillmäter dokumentationen mycket varierande betydelse. En del datoranvändare betraktar dokumentation av ett databehandlingssystem som en ganska ointressant fråga. De flesta tillmäter en fullgod dokumentation stor betydelse. Uppgifterna om tillgänglig dokumentation hos de intervjuade användarna varierar också. Många anser sig ha fullgod dokumentation medan andra både pekar på att den är bristfällig och att detta innebär sårbarhet.

Redan de första databehandlingssystemen ställde genom bl a den ökade komplexitet som präglar denna form av informationsbehandling nya krav på dokumentation av systemen. Behovet av dokumentation har sedermera ökat ytterligare i takt med utvecklingen av centrala integrerade system som mänsklig förmåga ej längre klarar överblicka utan tillgång till detaljerad dokumentation. Särskilt kanske behovet av dokumentation har gjort sig gällande i samband med övergång från en generation datorer till en ny eller vid byte till maskin av annat fabrikat liksom vid driftstörningar eller personalomsättning.

Behovet av dokumentation berör alla stadier av databehandling från planering och uppbyggnad av ett system via driften av detta till uppföljning och särskilda efterstudier av systemet eller de ändamål för vilket detta är skapat. Det är således inte bara fråga om den löpande driften; även arkivrutiner hör till denna fråga.

Även andra än de rent maskinella rutinerna behöver således numera dokumenteras. Kraven gäller också företeelser som blanketter, säkerhetsåtgärder, lokaler m m. I en fullständig dokumentation torde i dag även böra ingå katastrofplaner, i vart fall för databehandlingssystem av ett visst omfång.

Dokumentation omfattande
- initiering, kravspecifikation, förstudie etc
- detaljstudie med systembeskrivning etc
- nedbrytning av systemet
- programdokumentation
- driftdokumentation

torde allmänt sett vara ganska tillfredsställande i inledningsskedet av ett nytt databehandlingssystem. Undantag finns emellertid. Det torde dock vara ganska vanligt att de ofta fortlöpande förändringarna av systemen, av tidsskäl och ekonomiska orsaker, inte dokumenteras eller att det i vart fall inte sker på ett tillfredsställande sätt.

En del betraktar kostnaderna för en fullödig fortlöpande uppdaterad dokumentation som en försäkringspremie som bidrar till att undanröja eller begränsa kostnaderna i samband med skador och andra driftstörningar eller vid maskinbyten. Erfarenheter från exempelvis bränder i datacentraler eller övergången från IBM till Saab-datorer inom försvaret visar att detta synsätt med all sannolikhet är realistiskt.

Beroendet av dokumentation varierar beträffande olika system och användningssätt. Ett komplext integrerat centralt system som drivs i egen regi ställer varierande krav på dokumentation. Kraven beror dels på komplexiteten, dels på hur många och vilka som behärskar systemet. Vidare kan krävas dokumentation om andra system med vilka det egna systemet byter information. För att belysa detta kan hänvisas till en av Öhrlings Revisionsbyrå AB den 29 mars 1978 upprättad PM angående översiktlig genomgång av den interna kontrollen i det statliga löneadministrativa systemet SLÖR.

Då driften och utvecklingen av lönesystemet påverkas av flera myndigheter:
- Statskontoret (tv huvudman)
- DAFA, UDAC (driftställe)
- Användarmyndigheter

är det nödvändigt att ansvarsfördelningen mellan de olika myndigheterna är helt klarlagd.

Vi har inte kunnat klarlägga vilket ansvar t ex statskontoret i dag har när man centralt utanordnar medel för löneutbetalningar, utan att respektive myndighet först beordrat utbetalning av sina löner.

Inte heller har vi funnit några instruktioner om vilka kontroller DAFA bör utföra för att kontrollera riktigheten i löneberäkningarna, innan lönebanden sänds till PK-banken.

Det är synnerligen angeläget att bl a dessa frågor omgående löses i ett driftavtal.

Dessutom bör rutinerna mellan olika driftställen bl a vad gäller överföring av nya programversioner och tabelluppgifter formaliseras, i syfte att säkerställa att samma programversioner används vid alla driftställena.

Vidare sägs i detta PM om SLÖR som redan tagits i drift.

Den centrala dokumentationen är för närvarande inte komplett eller aktuell. Ett konsultföretag har fått i uppdrag att ta fram en dokumentation som i huvudsak motsvarar RAS-modellens krav.

Behovet av god dokumentation av systemets tekniska uppbyggnad och funktionssätt är påtagligt, då endast ett fåtal personer behärskar systemen.

Då dessutom såväl ett matrikelsystem som ett personaladministrativt system för bl a tjänster kommer att bygga på information från SLÖR förstärks kravet på god dokumentationsstandard.

I de fall in- och utdata ej är direkt avstämbara (avsaknad av audit trail) kan krav uppställas på systemdokumentation enligt bokföringslagen och den av bokföringsnämnden utfärdade anvisningen nr 3. (Motsvarande krav bör tillgodoses även av statliga system.)

Denna redogörelse gäller ett relativt enkelt löneutbetalningssystem. Sårbarheten i samband med t ex driftstörningar blir ganska begränsade. Erfarenheterna från andra system med högre grad av sårbarhet är emellertid desamma.

En annan dimension har bristen på dokumentation när användaren anlitar utomstående datorkraft. Är det fråga om ett standardsystem som tillhandahålls av servicebyråer är problemen dock mycket begränsade i händelse av driftstörningar, strejker, servicebyråns konkurs eller likvidation etc. I den situationen kan man vanligen utan tillgång till dokumentation anlita en annan servicebyrå eller överkapacitet vid någon annan datacentral. Råkar det däremot vara fråga om mera unika databehandlingssystem är risken stor att användaren blir strandsatt vid liknande händelser. Den informationsbehandling som sker kan försiggå i flera länkar i en kedja. Exempelvis kan en användare anlita redovisningscentraler eller bokföringsbyråer som i sin tur anlitar en servicebyrå. Denna kan vidare anlita samarbetande utländska företag. I en sådan situation saknar användaren vanligen tillräcklig dokumentation.

Dokumentationens betydelse framgår med all tydlighet av Anvisningar för utformning av dataskyddsåtgärder, som är en del av Datasäkerhetshandboken. Denna är framtagen av IBM Svenska AB inom ramarna för de datasäkerhetsstudier som bedrivits i Sverige åren 1974 — 77 av IBM i samverkan med bl a datainspektionen och statskontoret. I denna betonas vikten av fullgod användardokumentation, driftdokumentation, systemdokumentation och programdokumentation, som också måste hållas uppdaterad. En kopia av varje dokumentation bör arkiveras brandsäkert. Till detta kan fogas att dokumentation även bör förvaras på betryggande sätt för att förhindra dataintrång.

5.10 Katastrofberedskap

Det mest väsentliga för en katastrofberedskap är att katastrofplanering föreligger. Beredskapen omfattar dessutom kontroll av att utarbetade planer fungerar i praktiken.

Med katastrofplanering menas att förberedelser för katastrofsituationer vidtas och att i en katastrofplan dokumenteras vad som skall göras då en allvarlig skada eller störning inträffar.

Av SÅRKs intervjuarbete har i huvudsak följande framkommit. Endast hos några få av de tillfrågade hade utarbetats katastrofplaner. Någon större reservkapacitet utanför den egna huvudanläggningen fanns i regel inte. Ett mindre antal hade back-up avtal med andra

användare eller hade anslutit sig till ett särskilt konsortium i vilket de åtta medlemmarna gemensamt skaffat en reservlokal för datordrift. Lokalen är förberedd med ledningar för såväl elektricitet som för datakommunikation. En leverantör har utfäst att vid behov snabbt skaffa fram erforderlig maskinutrustning.

Flera av de intervjuade framhöll att det var svårt eller omöjligt att bara flytta över driften till annan anläggning och få det egna systemet att fungera och att svårigheterna ökade ytterligare om man var beroende av fungerande kommunikationssystem. Löpande parallelldrift var nästan en förutsättning för att en reservanläggning vid behov skulle fungera tillfredsställande ansåg flera.

De flesta hade back-up register i flera upplagor (generationer).

Vad gäller manuella back-up rutiner saknades sådana i de flesta fall. I den mån det fanns var det i regel inom någon begränsad sektor. Många framhöll att det nästan var omöjligt att ha några manuella rutiner. Ett av skälen som nämndes var att personalresurserna inte skulle räcka till. Det framhölls också att det var svårt att hålla olika manuella register aktuella, t ex ett lagerregister hos ett större företag med många driftställen.

Statskonsult AB har i rapport den 28 juni 1977, Katastrofplanering — en kartläggning, behandlat frågor av denna typ. I rapporten redogörs även för resultatet av en intervju med företrädare för åtta tekniskt avancerade datoranvändare inom förvaltning och näringsliv. Intervjuerna visade bl a att ingen av de intervjuade användarna hade utarbetat och dokumenterat någon katastrofplan.

I rapporten sägs att den välstrukturerade och väldokumenterade form av katastrofplanering som företrädesvis utländsk litteratur rekommenderar inte i någon nämnvärd utsträckning tillämpas av svenska datoranvändare.

I en amerikansk senatsrapport från 1976 rörande datorer[1] påtalas brister i katastrofplanering hos statliga datoranvändare. Vid inspektioner hos 28 olika användare visade det sig att endast 13 hade upprättat skriftliga katastrofplaner för att säkerställa driften om någonting skulle inträffa. Några inträffade händelser används för att illustrera behovet av katastrofplanering. Ett fall gäller en översvämning år 1972 som drabbade postverkets datacentral i Wilkes Barre, Pennsylvania. Postverket kunde fortsätta driften tack vare att katastrofberedskap fanns. Tidigare har nämnts — avsnittet om katastrofer och olyckshändelser — den brand som IBM råkade ut för och som bl a skadade företagets programbibliotek. Genom att företaget hade katastrofberedskap i vilket ingick katastrofplan lyckades man dock, trots stora skador, snabbt komma tillbaka till ett normalläge med rekonstruerat programbibliotek och full serviceverksamhet. Företaget framhöll efteråt att man haft stor hjälp av sin katastrofplan. Planen var av relativt enkel beskaffenhet. Det viktiga var att alla på förhand hade tvingats tänka igenom vad som skulle göras vid en eventuell katastrof. Detta betydde mera än själva dokumentet som innehöll katastrofplanen.

Inför utbytet av länsstyrelsernas datorer har länsstyrelserna framfört önskemål om biträde vid bestämmandet av krav på datorlokaler. Läns-

[1] Problems associated with computer technology in federal programs and private industry, Computer abuses. Washington 1976

styrelsernas organisationsnämnd (LON) och RSV bildade därför en arbetsgrupp som utarbetat en handledning inför planerandet av en datorcentral. I handledningen heter det beträffande katastrofplanering på följande sätt.

> Trots ett välorganiserat skydd av en datoranläggning finns risk för att en katastrof kan inträffa. — De regionala datorsystemen är till stora delar identiskt utformade varför driften i en nödsituation kan föras över till ett annat läns datoranläggning. En sådan överföring fordrar en noga genomtänkt och fastställdplan för att utan dröjsmål kunna igångsättas. — Planen bör förutom för ledning och samordning av verksamheten redogöra för eventuellt behov av manuella rutiner, liksom för återgång från manuella rutiner och drift på annan anläggning till normaldrift. Dessutom bör återanskaffning av utrustning, rekonstruktioner av register etc, vara planerad.

Det kan i detta sammanhang nämnas att det internationella betalningsförmedlingssystemet SWIFT körs på två parallella exakt likadana anläggningar förlagda till olika länder.

I katastrofplaneringen bör beaktas att olika åtgärder som möjliggör att driften på något sätt säkras t ex anskaffning av reservlokaler och reservutrustning samt framtagning av reservrutiner bl a manuella sådana. Vidare bör ingå back-up avtal med andra användare, kopior som möjliggör rekonstruktion av register vad avser såväl program som data, kopior av dokumentation etc. Själva planen bör i detalj reglera hur olika reservrutiner skall tas i anspråk, vilka system som skall prioriteras, hur personalen skall utnyttjas etc. Vidare bör i planen tas med handlingsprogram för återgång till normal drift.

Syftet med katastrofplanering är att om en allvarlig skada som stör datordriften inträffar så skall konsekvenserna av sådana skador motverkas och mildras så mycket som möjligt. Brister i katastrofplanering kan få förödande följder, åtminstone om skador inträffar i för samhället viktiga datasystem. Man kan anta — vilket även styrks av Statskonsults rapport och av SÅRKs intervjuundersökning — att katastrofberedskapen på många håll inte är vad den borde vara. Troligen är de myndigheter och organisationer som har en genomförd beredskapsplanering — vilken då även omfattar datorsidan — bäst rustade. Överväganden vid katastrof- och beredskapsplanering torde i stort vara likartade.

5.11 Utlandsberoende

5.11.1 *Allmänt*

Enligt SINDs rapport, skiljer sig datorindustrin väsentligt från övriga industrigrenar främst genom sin speciella marknadsföringsteknik, stora finansiella behov, en snabb teknologisk utveckling och mycket snabb tillväxttakt på marknaden. För att tillmötesgå dessa krav förekommer ett antal olika samarbetsavtal mellan olika datorföretag i världen. I rapporten redovisas vissa siffror som visar vilken dominerande ställning USA

har på världsmarknaden. Bl a framgår att amerikanska företags världsmarknadsandel den 1 januari 1974 var 90 % av totalt maskinvärde, medan de europeiska och japanska företagens andelar uppgick till 5 % vardera.

Några färskare siffror redovisas även i rapporten. Det sägs bl a att marknaden domineras av ett fåtal amerikanska företag, att IBM under 1976 vad gäller generella datorer och datasystem svarade för ca 58 % av världsmarknaden och att de sex största amerikanska datorföretagen tillsammans svarade för över 80 % av världsmarknaden.

Av rapporten framgår vidare att den totala försäljningen av datamaskinvaror i Sverige under 1975 uppgick till 1 830 miljoner kronor och 1976 till 2 320 miljoner kronor. Vad gäller saluvärdet av den totala inhemska produktionen av datamaskinvaror uppgick den under 1975 till 1 540 miljoner kronor och 1976 till 1 720 miljoner kronor. Den inhemska produktionen är emellertid inriktad mot ett relativt begränsat antal varor. Några utmärkande drag hos den inhemska produktionen redovisas i rapporten på i korthet följande sätt

- Den svenska produktionen av centralenheter består uteslutande av mindre kontors- och minidatorer. Produktion av generella datorer förekommer inte längre.
- Produktionen av periferienheter, exkl terminaler, består huvudsakligen av skrivare och hålremsprodukter.
- Den inhemska produktionen av terminaler, som värdemässigt är av samma storleksordning som den totala tillförseln, domineras av bankterminaler. Även produktionen av generella bildskärmsterminaler är betydande.
- Produktionen av datakommunikationsutrustning består huvudsakligen av modem.

SÅRK noterar dessutom att en betydande tillverkning av specialiserade datorer för programstyrda televäxlar vuxit fram under de senaste åren.

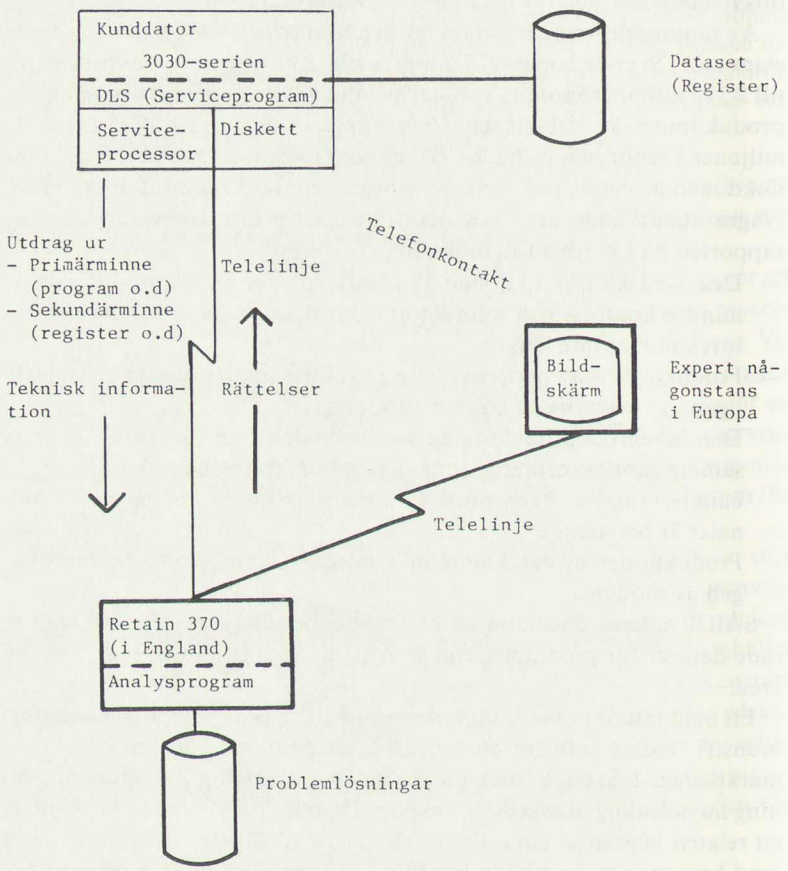
Ett ökat internationellt samarbete kan alltså skönjas vad gäller datorindustri. Vidare framgår att USA har en dominerande roll på världsmarknaden. I Sverige förekommer en inte obetydlig inhemsk tillverkning huvudsakligen avsedd för export. Denna tillverkning är inriktad på ett relativt begränsat antal varor. Detta gör att Sverige likafullt är i hög grad beroende av andra länder. Bl a är vi beroende av import av större datorer och elektroniska komponenter. Frågan är i vad mån Sverige kommer att kunna följa med i den snabba tekniska utvecklingstakten. Redan i dag har USA betydande försprång beträffande halvledarteknik m m. Ett ökat importberoende kan vara att vänta även beträffande mindre datasystem.

5.11.2 *Drift, underhåll, service, reservdelar och transport*

I den mån man är beroende av import av datasystem eller delar av sådana system finns även utlandsberoende beträffande drift, underhåll och service men även utbildning. Även om det finns en relativt omfattan-

de expertis inom landet är det inte säkert att den alltid räcker till. De leverantörer SÅRK har tillfrågat ansåg att det finns relativt goda resurser för service inom landet. Det kan i detta sammanhang nämnas att IBM håller på att utveckla ett system som kallas Remote Support Facility, se bild.

Remote support facility (RSF)



Detta innebär att en speciell dator placerad i England sätts i förbindelse med kunddatorer via telelinje. Den speciella datorn skall förses med information från kunddatorn om något fel inträffar i den. Genom bearbetning av informationen skall felet kunna lokaliseras. Informationen om hur rättelse skall ske kan sen sändas via telenätet. En expert någonstans i Europa skall via bildskärm ombesörja bearbetningen och se till att underlag för rättelse tas fram. Man får räkna med att experter av detta slag utgör en relativt begränsad skara. Även andra leverantörer håller på att utveckla liknande system.

Vad gäller reservdelsförsörjningen har frågan behandlats av försörjningsberedskapsutredningen i SOU 1975:57 Varuförsörjning i kristid. Utredningen säger vad gäller utrustning för numerisk styrning, processstyrning och annan produktionsstyrning bl a följande.

Automatiserade system för styrning av processer kan ha olika karaktär — från styrning av vissa sekvenser av en tillverkningsprocess till avancerade system där en mindre dator övervakar och ingriper i hela processen. Processtyrsystem används särskilt inom kemisk industri, massa och pappersindustri samt järn-, stål- och metallverk. Ca 15 företag har ansett att tillförseln av komponenter till elektronisk styrutrustning av denna typ kan vara ett särskilt känsligt område i ett avspärrningsläge. — Med hänsyn till att processtyrutrustningen används i industrier där produktionen i en viss punkt i varje ögonblick är beroende av att närmast föregående tillverkningsmoment fungerar kan avbrott i reservdelstillförseln för denna typ av utrustning dock bedömas få allvarligare konsekvenser än vad som gäller för NS-maskiner (numeriskt styrd utrustning). — Gemensamt för de olika varianter av utrustning som här diskuteras är att de innehåller ett elektroniskt styrsystem. Det är reservdelsförsörjningen för sådana system som företagen i stor utsträckning bedömt vara känslig. — Produktion av färdiga styrsystem förekommer hos flera svenska företag som t ex ASEA, SMT och DATA-SAAB. Vid tillverkningen utgår man från halvledarkomponenter som sätts samman i olika kombinationer till kretskort. Av dessa byggs därefter den elektroniska styrenheten upp. Huvudproblemet har bedömts vara försörjningen med halvledarkomponenter. Två svenska företag är verksamma på detta område — AB Rifa som är ett dotterföretag till LM Ericsson samt ASEA-HAFO AB. Rifa tillverkar integrerade kretsar, kondensatorer och andra speciella elektronikkomponenter. HAFO är bl a inriktat på framställning av integrerade kretsar, speciella transistorer, termistorer och andra speciella komponenter. Den svenska produktionens andel av tillförseln är liten. Den internationella handeln på detta område domineras av några USA-företag som framställer alla de 1 000-tals varianter som förekommer av dessa elektroniska komponenter. Den svenska produktionen omfattar endast en mindre del av dessa. Sortimentet kan i viss mån breddas i ett krisläge men detta kan givetvis ske först efter viss tid. Det är på grundval av denna översiktliga undersökning svårt att avgöra i vilken utsträckning inhemsk ersättningsproduktion kan ersätta de importerade komponenterna. Vissa minneselement bedöms överhuvudtaget inte kunna framställas inom landet. Lagerhållningen av reservdelar hos företag som använder NS-och processtyrutrustning är i regel obetydlig då man förlitar sig på leverantörernas service. — Vid kontakter med de företag som ingår i enkätundersökningen och tillverkare av styrutrustning respektive halvledare har det framkommit att elektroniska komponenter i meningen halvledare, kretskort etc är mycket hållbara. De fel som uppkommer inträffar normalt under den första tiden efter det att utrustningen tagits i bruk. Det är därför numera vanligt att komponeterna konståldras (bränns in) av tillverkarna, varigenom driftsäkerheten avsevärt ökar.

Beträffande datorer i allmänhet sägs bl a

Utredningens enkätundersökning har avsett reservdelsförsörjningen för industrins direkta produktionsutrustning. Datorer i allmänhet har således inte behandlats, dock med undantag av sådana som ingår i utrustning för processtyrning och annan avancerad styrutrustning. Vi har emellertid ansett att reservdelssituationen även på detta område bör beröras. Anledningen härtill är givetvis samhällets numera starka beroende av datortjänster och de med tiden allt större svårig-

heterna att övergå (återgå) till andra (gamla) metoder för informationsbehandling. — ÖEF har i en särskild utredning som företogs åren 1971 — 72, Data under beredskap och krig (DBK 71) behandlat beredskapsförhållandena på främst ADB-området. Denna utredning bedömde på basis av en enkätundersökning hos olika datoranvändare möjligheterna att ersätta datorer med ickemaskinella rutiner eller genom att använda andra anläggningar. Frågeställningarna i enkäten var av sådan karaktär att endast en ungefärlig uppskattning av datorberoende kan göras. Det torde emellertid stå klart att möjligheterna till omställningar är små. Således angav endast 14 % av tillfrågade industriföretag och 12 % av handels- och serviceföretagen att ADB-användningen i sin helhet skulle kunna ersättas med andra rutiner. Dessa frågor avsåg ett krigsläge men är av intresse även i ett vidare perspektiv. Av enkätsvaren framgår vidare att ADB-beroendet efter hand bedöms öka ytterligare. — Utgångspunkten för vår översiktliga behandling av reservdelsproblematiken på datorområdet är att det befintliga datorbeståndet till övervägande del måste antas behöva fungera i normal drift även i ett krisläge. Frågeställningen blir då om svensk industri har kapacitet att ersätta de delar, tillbehör och komponenter som normalt förslits i datorer och kringutrustning och om underhållet av maskinparken kan upprätthållas i tillräcklig omfattning. — De bedömare som vi varit i kontakt med anser att komponentförsörjningen kommer att bli det allvarligaste problemet vid av avspärrning. De komponenter det här är fråga om är av i princip samma slag som sådana vilka används i de styrutrustningar som behandlas i föregående avsnitt. Det resonemang som förs där är således tillämpligt även då det gäller försörjningen med komponenter till datorer för ADB-användning. — Maskinleverantörerna håller vissa reservdelslager i Sverige. De multinationella företag det här är fråga om har en hierarkiskt organiserad reservdelslagring så att enklare och frekventa delar lagras hos större kunder medan vissa av de reservdelar som erfordras i Sverige och som sällan behöver ersättas förrådshålls i ett svenskt centrallager. Övriga delar finns lagrade på ett fåtal platser i Västeuropa. — Ifråga om underhåll är detta från de stora maskinleverantörernas sida organiserat på samma hierarkiska sätt som reservdelslagringen. Två svenska företag, SRA och Telub är dock verksamma på detta område, i första hand vad gäller mer ovanliga maskinfabrikat. — Tillbehörsfrågan bedöms vara ett något mindre problem än komponenterna. Papper till hålkort importeras visserligen för närvarande men kan ersättas med svensk vara. Magnetband och skivpackar tillverkas inte i Sverige. Det är osäkert om det inom landet går att åstadkomma beläggningen på banden men de band som finns kan slitas avsevärt längre tid än vad som sker under normala förhållanden. Svensk verkstadsindustri uppges på sikt böra kunna klara en tillverkning av skivpackar. — Programvara slutligen är en fråga om kompetens och utbildning hos personal och Sverige anses vara ganska väl utrustat på detta område. — Sammanfattningsvis kan konstateras att reservdelssituationen kan vara relativt bekymmersam på datorområdet. Det svåraste problemet utgör elektroniska och elektromekaniska komponenter. Lagring förekommer genom maskinleverantörernas försorg men som redan nämnts gäller detta inte alla delar. Enligt DBK 71 uppgavs lagringen av de mest förbrukade delarna till 4 — 6 månader. De inhemska produktionsmöjligheterna diskuteras i föregående avsnitt. — Om en ej obetydlig del av datorbeståndet inte anses behöva vara i drift i ett krisläge uppstår möjligheter att byta delar mellan maskiner vilket påtagligt kan öka uthålligheten. I viss utsträckning kan även delar tas från datorer för ADB-användning till sådana som används för produktionsstyrning.

I SINDs rapport heter det att den övervägande delen av tillförseln av halvledare kommer genom import. Med tillförsel menas då produktion

och import minskat med export. SIND framhåller att importens andel av den totala tillförseln varierar kring 100 %. Vidare sägs att produktionens andel av tillförseln som är ett grovt mått på självförsörjningsgraden ligger vad gäller integrerade kretsar kring 10 % och beträffande diskreta halvledarkomponenter kring 20 %.

Vid SÅRKs intervjuer har användarna som svar på frågan om hur lång tid ADB-verksamheten skulle fungera efter en total avspärrning — i de fall de överhuvudtaget ansett sig kunna svara — givit högst varierande uppgifter. De tider som har nämnts har legat mellan 2 — 3 månader och 2 år. De mest optimistiska har pekat på möjligheterna att reparera i större utsträckning och att i vissa fall kunna plocka delar från andra maskiner framförallt i ett krigsläge när viss ADB-verksamhet måste upphöra. Några leverantörer har även tillfrågats. En del av dessa nämnde att man i högre grad än i dag skulle reparera delar i stället för att byta ut dem. Ett par leverantörer räknade med att reservdelslagren för de viktigaste funktionerna skulle räcka några månader. En leverantör angav en lagerhållning i Sverige som värdemässigt motsvarar 24 månaders förbrukning vad gäller reservdelar. Detta garanterade emellertid inte beredskap för lika lång tid. Även leverantörerna pekade på möjligheten att plocka delar från datorer i mindre viktiga system. En leverantör trodde att det största problemet vid en avspärrning var att få fram förbrukningsmateriel, där inhemsk produktion saknas och där det skulle ta lång tid att få igång en sådan.

När man tar upp frågan om utlandsberoendet bör även beroendet av ett fungerande transportväsende nämnas. En förutsättning för att maskiner, reservdelar, halvfabrikat och komponenter av olika slag skall kunna importeras är att transportväsendet fungerar. Transport av databärare sker till stor del med bil, järnväg och flyg. Avbrott i teleförbindelser kan medföra att data behöver transporteras med mera traditionella medel.

5.11.3 *Leveranser av in- och utdata, bearbetningar utomlands*

Sedan länge förekommer ett mycket stort internationellt dataflöde. Magnetband och andra databärare sänds över gränserna. Telekommunikationstekniken har möjliggjort allt enklare och snabbare massöverföring av data. Som några variationer på dataflöde över gränserna kan nämnas

- data i form av listor, mikrofilm etc översänds på traditionellt sätt
- data lagrade på maskinläsbart medium översänds på traditionellt sätt
- datalagrad information överförs via fast uppkopplade eller uppringda ledningar i telenät eller datanät via kabel eller satellit från terminal till dator eller från dator till dator.

I Sverige har ett allmänt datanät tagits i drift. Detta skall sedan sammankopplas med ett nordiskt datanät. Även i andra länder finns eller planeras allmänna datanät. De olika nationella allmänna näten kan förutsättas bli sammankopplade. Åtskilliga internationella privata nät finns redan. Som exempel kan nämnas SWIFT-systemet inom banksektorn till vilket de flesta svenska affärsbanker anslutit sig.

Dataflödet över gränserna är av samma slag som flödet inom ett land. Datatransmission används således för bl a

- att bearbeta information och sedan återföra bearbetningsresultatet eller delar därav
- att bearbeta information samt både slutligt lagra den utomlands och återföra bearbetningsresultatet eller delar därav
- att samköra egen information med information i data banker i ett eller flera andra länder och återföra bearbetningsresultatet eller delar därav.

Användare av internationell dataöverföring finns i första hand inom näringslivet. Det finns dock även exempel på myndigheter som utnyttjar datorer utomlands.

På den privata sektorn förekommer internationellt dataflöde inom de flesta verksamheter. Som exempel kan nämnas flygbolagen, oljebranschen, kreditkortsföretag och leasingfirmor, radio- och TV-branschen, bilproducenter, läkemedelsindustrin, banker och försäkringsbolag. All slags information ingår. Även om flödet av persondata är stort torde det dock mest vara fråga om tekniska och ekonomiska data.

Även på den offentliga sektorn dominerar flödet av tekniska och ekonomiska data. Persondataflöde förekommer i huvudsak när det är fråga om internationellt samarbete. Inom Interpol diskuteras för närvarande ett ADB-system med datakommunikation. Andra exempel är den internationella meteorologiska trafiken, uppgifter om patent m m.

Inom Malmö kommun förs ett register benämnt brandkårens riskregister. Detta register bearbetas i USA och in-och utdata sänds via det vanliga telekommunikationsnätet.Ändamålet med detta register är att vid larm tillhandahålla utryckningsstyrkan aktuella beskrivningar över risker m m på larmplatsen. I registret ingår för närvarande ca 250 företag med automatiskt brandlarm inom Malmö kommun. När automatiskt larm utlöses hos brandkåren startas ADB-bearbetningen i en dator belägen i Cleveland, Ohio, USA. Brandkårens terminalskrivare framställer utskrift av registrerade uppgifter om det aktuella företaget. Det gäller bl a uppgifter om byggnader, vattentillgångar, avstängningar av el, gas och vatten samt speciella risker som förekomst av olika kemikalier.

Flera servicebyråer i Sverige förmedlar tjänster som innebär bearbetningar utomlands. Genom att kunder finns i hela världen kan man dra ekonomisk nytta av tidsförskjutningen. Följande exempel på denna typ av service ges i SINDs rapport.

Servicebyråer erbjuder via sina datanät datakraft till sina kunder. Servicebyråerna hyr av teleadministrationerna höghastighetsförbindelser mellan datacentral och lokalt placerade koncentratorer, dit byråns kunder ansluts. — General Electric's (GE) MARK III nät täcker USA, Västeuropa, Japan och Australien. Den transkontinentala datatrafiken går via satelliter. Den europeiska delen av nätet består av en central koncentrator i London som i sin tur förbinder ett antal lokala koncentratorer i övriga Europa, varav en i Stockholm. MARK III är ett stjärnnät, dvs alla förbindelserna leder till en central punkt. Denna ligger i Cleveland, USA och inrymmer en gigantisk datacentral med ca 25 datorer. Via nätet kan GEs kunder köpa en rad olika databehandlingstjänster. I Europa marknadsförs

MARK III-tjänsterna av Honeywell-Bull Information Services. — Control Data Corporation (CDC) erbjuder databehandlingstjänster via Cybernet. Nätet täcker Nord- och Sydamerika, Europa och Australien.

Ett förhållande som också bör uppmärksammas är att flera servicebyråer har avtal om back-up i annat land. Detta innebär att t ex redovisning för många företag kan databehandlas utomlands utan att företaget i fråga känner till detta.

I en rapport den 1 april 1978 har Logica Ltd, London, på uppdrag av OECD, behandlat användandet av internationella datanät. I rapporten redovisas bl a följande slutsatser.

- Användandet av internationell dataöverföring har medfört påtagliga ekonomiska fördelar för stora multinationella företag, flygbolag och banker
- ett av de viktigaste skälen till att datanät har skapats och ett av de viktigaste skälen till att dataöverföringar sker är att datorresurserna härigenom kan delas
- många företag som har dragit nytta av fördelarna av internationella dataöverföringar har i sådan grad ändrat sina rutiner att de är beroende av fortlöpande tillförlitlig service. Som exempel nämns flygbolagen
- internationell databearbetning och dataöverföring ökar det internationella beroendet, dock att vissa risker kan minskas med hjälp av datanät med möjlighet till omkopplingar
- ett allmänt europeiskt datanät kommer troligen inte att vara uppbyggt tidigare än om fem år
- användningen av internationella datanät hänför sig i huvudsak till administration av företag, till bankväsendet, kreditkontroll och till bokning av resor
- vissa multinationella företag har lagt upp centrala register med information rörande alla sina företag. Detta betyder att data som rör driften av industriföre tag inom ett land finns utanför landets gränser.

Sammanfattningsvis kan följande sägas. Behovet av komponenter, reservdelar, service från utlandet m m gör vårt land beroende av att det internationella handelsutbytet flyter utan allvarligare störningar. Man kan utgå från att vår reservdelslagring, våra möjligheter till egen tillverkning och våra möjligheter till inhemsk service skulle möjliggöra datordrift i nuvarande omfattning endast under kortare tid om störningar skulle uppstå på grund av krig, avspärrningar, handelsblockader o d. Det finns skäl att anta att det beroende som nu diskuteras kommer att öka.

Det ökade dataflödet över gränserna medför säkerhets- och sårbarhetsproblem av andra dimensioner än de som finns om man ser endast på rent nationella förhållanden. Om databehandlingen sker på en dator som finns i ett annat land eller på en annan kontinent, och om in- och utdata skall passera genom flera länder ökar därmed även riskerna för angrepp av olika slag. Att skydda sig mot händelser utom riket är av

naturliga skäl svårare än att bygga upp ett inhemskt skydd. Utvecklingen pekar mot att internationella datanät — såväl allmänna som privata — kommer att bli vanligare. Därmed kommer också dataflödet att öka.

III Fortsatt kartläggning

6 Revidering och komplettering föranledd av det fortsatta arbetet och remissinstansernas påpekanden

I lägesrapporten har SÅRK uttalat att ytterligare kartläggning skall ingå i det fortsatta utredningsarbetet. Några omfattande kompletteringar har SÅRK inte funnit erforderliga. Det som nu redovisas bygger delvis på synpunkter och material som tillförts genom remissvaren på SÅRKs lägesrapport.

6.1 Kommunikationsteknik

I lägesrapporten har SÅRK i ett särskilt avsnitt (kap III) behandlat kommunikationsteknik. Kapitlet bygger huvudsakligen på en konsultrapport av Teleplan AB.

Några remissinstanser har understrukit datakommunikationernas betydelse vid en värdering av sårbarheten. Bl a har framhållits vikten av att det allmänna datanätet utformas på ett sätt som ger låg sårbarhet t ex genom decentraliserade lösningar. En remissinstans har även efterlyst en sårbarhetsbedömning vid användning av kommunikationssatelliter. Vid remissbehandlingen har även den åsikten förts fram att vinsterna från sårbarhetssynpunkt med decentraliserade systemlösningar till stor del kan gå förlorade om man i allt för hög grad förlitar sig på datakommunikation.

SÅRK delar helt uppfattningen att den ökade användningen av datakommunikationsteknik måste tillmätas stor betydelse vid bedömning av sårbarhetsfrågor.

När det gäller det allmänna datanätet har televerket ställt ett antal krav för att nå högsta möjliga tillgänglighet i nätet. Bl a har följande krav påverkat uppbyggnaden

- hög kvalitet på komponenterna i nätet
- dubblering av centrala utrustningar och förbindelser mellan dem
- automatisk övervakning av utrustningar och förbindelser
- omkoppling till reservenheter och alternativa förbindelser vid fel
- automatisk felavgränsning och fellokalisering
- automatisk dirigering av larm och felutskrifter till rätt drift- och underhållsställe.

Beträffande det nordiska allmänna datanätet har från början installerats en växel i vardera av de fyra nordiska huvudstäderna. Under 1980-talet kommer emellertid ytterligare ett tiotal växlar att införas varav

fyra på olika platser i Sverige, en spridning som måste anses positiv från sårbarhetssynpunkt.

Det kan även nämnas att televerket tillhandahåller olika tilläggstjänster i form av kontroll och spärrmöjligheter för abonnenten. Kunden kan alltså själv bedöma hur stor säkerhet hans system kräver i överföringsledet och med utgångspunkt från detta bestämma vilka tilläggstjänster av dataskyddskaraktär han önskar.

När det gäller påståendet att decentraliserade systemlösningar kan medföra ökad sårbarhet genom ökat beroende av datakommunikationer vill SÅRK anföra följande. Detta är en fråga som sammanhänger med frågan om vilken verksamhet som skall använda ett ADB-system, där bl a behov av riksåtkomst m m kommer in i bilden. I de fall då man kan förlägga huvuddelen av information och bearbetningar nära användarna och då behovet av informationsutbyte med andra delar av organisationen på regional eller central nivå är litet, minskas behovet av datakommunikationer. Är däremot behovet att byta information stort och finns krav på att snabbt få fram rikstäckande information från en mängd olika organisationsenheter blir bilden en annan. När sådana krav ställs kan kommunikationsdelen bli mera komplicerad och sårbar vid decentraliserade lösningar, än vid centraliserade. Vad som är den bästa totala lösningen får naturligtvis avgöras i det enskilda fallet. Något som i vart fall bör undvikas är onödigt komplicerade knytningar inom eller mellan olika system.

Kommunikationer över satellit är något som alltmer kommer till användning främst i den internationella datatrafiken. För svenskt vidkommande torde satellitkommunikation komma att ingå i bilden så gott som uteslutande vid dataflöden över gränserna. Inom den närmaste framtiden lär dock andra kommunikationsmedel i första hand komma till användning. Vissa internationellt och även i Sverige verksamma servicebyråer med datorkapacitet i olika delar av världen använder och kan i ökande omfattning tänkas använda satellitöverföringar. I lägesrapporten har SÅRK inte närmare diskuterat sårbarhetsproblem som hänger samman med sådana överföringar. Endast känsligheten för EMP-effekter har nämnts.

Satellitöverföring behandlas i SINDs rapport datamarknaden inför 1980-talet. Där heter det bl a att kommunikation över satellit under 1980-talet kan komma att medföra betydande förändringar såväl vad gäller transmissionskostnad som nya kommunikationsmöjligheter. Det företag som leder utvecklingen på detta område är Satellite Business Systems (SBS). SBS avser att inom ramen för ett gemensamt kommunikationssystem överföra tal, data, textvideo och faksimil. SBS utnyttjar inte i någon del av kommunikationsvägen markbundna ledningar och information går direkt från användare till användare. Under 1980-talet kan SBS och andra liknande system komma att erbjuda sina tjänster till Europa heter det i rapporten. Om man i Europa inte har utvecklat motsvarande tjänster kommer starka krav att resas från europeiska företag att få utnyttja de amerikanska systemen. Detta skulle påverka de europeiska teleförvaltningarnas monopolställningar. Enligt

rapporten skulle en sådan utveckling sannolikt få politiska konsekvenser i flera avseenden. Det sägs att ur såväl social- som ekonomisk- och försvarspolitisk synvikel är telekommunikationen en resurs som ett land måste ha full kontroll över.

Frågan om satellitöverföringar hänger nära samman med i vad mån bearbetningar av känslig information bör ske utomlands. I denna del har SÅRK uttalat att beträffande ADB-bearbetningar utomlands bör det vara ett svenskt intresse att sådana inte sker helt utan kontroll och att för vissa typer av data eller vissa funktioner är sårbarhetsriskerna så framträdande att utlandsbearbetningar inte bör förekomma. I den mån man tillåter sådana bearbetningar torde överföringssättet vara av underordnad betydelse. Satellitöverföring kan för övrigt användas som reserv t ex om man av någon anledning behöver hoppa över ett land. Sådan överföring är billig, flexibel och ger stort kanalutbud samt är dessutom relativt svår att avlyssna. När det gäller satellitöverföringar kan dessa i framtiden få konkurrens av överföringar i fiberkabel (optisk fiber), en teknik som för närvarande håller på att utvecklas. Fiberkabel har hög överföringskapacitet och goda överföringsegenskaper. Sådana överföringar är nästan omöjliga att avlyssna samt mycket svåra att störa.

Slutligen vill SÅRK när det gäller frågor om datakommunikation även peka på en del faktorer som är av mer allmängiltigt slag. En inte helt ovanlig företeelse är som nämnts att system görs onödigt komplicerade genom att krav ställs på snabba informationsflöden i systemen eller mellan olika system utan att behovet är särskilt starkt. Många gånger kan informationen hämtas från annat håll eller i vart fall på annat sätt utan att servicegraden nämnvärt behöver sänkas. Däremot kan man uppnå betydande vinster från sårbarhetssynpunkt med sådana lösningar. Man kan säga att det i många fall skapas ett beroende av informationsutbyte och därmed datakommunikationer som är mer eller mindre onödigt. Det gäller att väga för och nackdelar med olika lösningar och att försöka undvika sådana där nackdelar t ex i form av ökad sårbarhet starkt överväger fördelarna.

Även när det gäller datakommunikation är det viktigt att olika användare har olika reservmöjligheter och inte minst en väl genomtänkt katastrofplanering.

6.2 Innehållsmässigt känsliga register och funktionellt känsliga användningsområden

6.2.1 *Vissa kompletterande uppgifter*

SÅRK har i avsnitt 5.1 och 5.2 ovan redogjort för ett antal olika innehållsmässigt känsliga register och funktionellt känsliga ADB-användningsområden. Vidare har SÅRK påvisat hur ansamling av stora datamängder sker och hur dessa kan användas för andra syften än de ursprungliga t ex i underrättelseverksamhet. I remissvaren finns vissa ytterligare exempel inom nu berörda områden som kan vara värda att relatera.

LMV har redogjort för olika tillämpningsområden för LMVs datasystem. Dessa är bl a

— Riksnäten (De nät varav vårt lands geodetiska stomme är uppbyggd. I riksnäten finns alltså grunddata med lägesbestämningar, höjdbestämningar m m)

Rikstrianguleringar (Lägesbestämning sker genom uppmätningar av vinklar och längder i ett geometriskt system ursprungligen ofta utformat som ett nät av trianglar; därav triangulering)

Rikets höjdnät (Tas fram genom höjdmätning. Höjdbestämning utförs i regel genom avvägning. Härigenom bestäms i första hand höjskillnaden mellan på marken fixerade punkter)

Rikets tyngdkraftsnät (I detta ingår tyngdkraftsdata vilka bl a kan användas för s k tröghetsnavigering bl a vad gäller robotar, flygplan, fartyg och undervattensbåtar)

Astronomisk ortsbestämning (Ortsbestämningen sker genom mätning mot olika himlakroppar)

— Vetenskaplig geodesi
— Geodetiska data i uppdragsverksamhet
— Allmänna kartläggningen
— Kartdata i uppdragsverksamheten
— Skogsvärdering
— Flygfältsdata
— Höjddata
— Markdata i fysisk planering, fritidshusinventering, fastighetsdata m m (Användning, beskaffenhet osv)

LMV säger att beträffande vissa geodetiska data uppmärksammas normalt inte deras underrättelsevärde. Enligt LMV kan triangelpunkter, tyngdkraftsdata och höjddata utnyttjas för ledning av indirekt eld. På senare tid märks särskilt utvecklingen av kryssningsrobotar, vilka styrs bl a med stöd av i robotarna datalagrad landskapsinformation. Geodetiska data som lagras i databaser är från underrättelsesynpunkt så viktiga att de inte bör lämnas ut utan särskild prövning. Kartor och flygbilder kan innehålla uppgifter om olika försvarsanläggningar samt vissa anläggningar inom det övriga totalförsvaret. Den moderna tekniken medger datalagring i stor mängd av uppgifter i kartor och flygbilder framhåller LMV.

Enligt LMV är svårigheten att skydda hemliga uppgifter inom bl a området för landskapsinformation betydande i och med att informationen kan hanteras med hjälp av ADB. Innehållet i lantmäteriets olika register kan underlätta för främmande makt att tillvarata, utvälja och sammanställa information av sådan art som är av betydelse från underrättelsesynpunkt, säger LMV, och tillägger att riskerna ökar inom lantmäteriet på grund av att datoriseringen ökar.

Det kan även nämnas att regeringen tillkallat en särskild utredare (Bo 1978:08) med uppdrag att utreda lantmäteriets uppgifter att tillhanda-

hålla information om landskapet. I direktiven till utredaren framhålls denna informations stora betydelse för samhällsplaneringen. Vidare räknas ett antal olika myndigheter upp som i dag svarar för produktionen av landskapsdata. Enligt direktiven bör den särskilde utredaren närmare överväga vilka uppgifter lantmäteriet bör ha som producent, samordnare och distributör av landskapsinformation. Utredarens arbete bör, enligt direktiven, syfta till att åstadkomma en effektiv organisation och rationella arbetsformer för insamling och behandling av landskapsinformation. Även användning av datateknik skall studeras. Uppdraget går alltså i korthet ut på att studera hur man, med bl a hjälp av ADB-teknik skall kunna samla in, lagra och bearbeta samt distribuera lägesbestämd landskapsinformation på ett rationellt, effektivt och samordnat sätt, till fromma för samhällsplaneringen. Även sårbarheten berörs i direktiven såtillvida att utredaren i sina överväganden bör beakta att landskapsinformation måste kunna tillhandahållas också under kris- och krigsförhållanden. Vidare sägs att behovet av sekretessgranskning av kartor och annan landskapsinformation bör beaktas.

Vägverket anför i sitt remissyttrande att bland de tekniska ADB-systemen finns vägdatabanken, vilken är av speciellt intresse genom att den innehåller grundläggande uppgifter om vägnätet, broar etc. Även koordinatuppgifter för vissa punkter på vägnätet samt för broar finns lagrade i vägdatabanken. Kopior av vissa delar av vägdatabanken finns hos andra statliga institutioner, t ex CFD, samt privata företag. Företagen utnyttjar, enligt vägverket, uppgifterna för datorstödd transportoptimering. I detta sammanhang kan nämnas att större vägtransportföretag även använder ADB-teknik för att optimera användningen av lastutrymmena alltså för att i görligaste mån undvika att bilarna går tomma. Störningar i ADB-driften kan alltså även medföra störningar i olika transportkedjor.

Vägverket anser att av de uppgifter som finns i vägdatabanken är koordinatdata och brodata de känsligaste från sårbarhetssynpunkt.

I lägesrapporten har SÅRK diskuterat de risker från sårbarhetssynpunkt som kan sammanhänga med användningen av de koordinater som finns i inskrivnings- och fastighetsregistren bl a genom de koordinatsatta personbanden och vidareanvändningen av dessa. CFD har i sitt yttrande ifrågasatt om de risker SÅRK pekat på har någon relevans. CFD menar bland annat att det koordinatsatta personbandet i stort sett är en kopia av länsstyrelsens personband utan något ytterligare informationsinnehåll. Den väsentliga skillnaden är dock, enligt SÅRKs mening, att genom att personinformationen med hjälp av koordinaterna kan lägesbestämmas på lägsta administrativa nivå har man ett utmärkt hjälpmedel att kartlägga var olika grupper av människor finns. De koordinatsatta personbandet i sig är heller inte speciellt intressanta i detta sammanhang. Det väsentliga är vad de koordinatsatta personbanden används till och kan användas till genom samkörning med andra register.

CFD har även angivit lagringstekniken — magnetband — och att det koordinatsatta personbandet endast uppdateras en gång per år och

dessutom inte är tillgängligt från terminal som ytterligare skäl för att sårbarhetsriskerna skulle vara låga. Emellertid framgår av ett nyligen avgivet systemförslag att den tekniska organisationen nu förändrats med övergång från magnetbandsorienterat system till direktminnesorienterat.

Såsom närmare utvecklas under avsnitt 8.3.1 nedan har en kommitté nyligen tillkallats för att närmare utreda hur fastighetsdataprojektet skall slutföras. Kommittén skall bl a beakta sårbarhetsfrågor.

Utöver de funktionellt känsliga områden som nämnts i avsnitt 5.2 bör även nämnas den grafiska industrin, som blivit alltmer datoriserad. Den nya tekniken har redan nått våra dagliga tidningar och sprider sig till många andra användningsområden. Vad gäller tidningar kan man här i förlängningen tänka sig en utveckling mot elektroniska tidningar. Dessa kan man då bläddra i med användning av skrivmaskinsterminal eller bildskärm med möjlighet att framställa papperskopior med hjälp av faksimilutrustning.

I sitt remissvar över SÅRKs lägesrapport har beredskapsnämnden för psykologiskt försvar framhållit, att i ett läge av kris och krig har massmedierna, inte minst pressen, en viktig uppgift inom det psykologiska försvaret. Nämnden har med oro noterat att pressen i ökad grad blivit beroende av ADB-teknik både när det gäller grafisk produktion och administrativa rutiner.

6.2.2 *Användning av kryptering och av behörighetssystem*

Vid remissbehandlingen har framförts synpunkter beträffande möjligheterna att med kryptering och behörighetssystem minska sårbarhetsriskerna vad gäller innehållsmässigt känsliga system. Kryptering av data sker genom att läsbara data omvandlas till icke läsbara data. Omvandlingen sker vanligtvis med hjälp av en beräkningsprocedur (algoritm) styrd av en krypteringsnyckel. I regel hemlighålls endast krypteringsnyckeln men det är möjligt att hemlighålla även algoritmen. Med tanke på standardiseringssträvanden är det mindre lämpligt att hemlighålla krypteringsalgoritmen. Det är tvärtom av stort värde att kunna använda samma algoritm för ett stort antal tillämpningar. I USA används en standardalgoritm, främst av federala myndigheter, sedan hösten 1976. Det finns även andra tekniska möjligheter att skydda information t ex genom att s k filsplittring används. Detta innebär att känsliga uppgifter lagras i ett register och identitetsuppgifterna i ett annat. Med en kod kan de båda registren sedan knytas ihop. Användning av kryptering har diskuterats bl a i integritetsskyddssammanhang. I SCBs utredningsrapport 1976-03-08, Förstöring, avidentifiering och kryptering, framhålls att kryptering ofta ger ett gott skydd mot obehörig åtkomst men att användningen av kryptering även medför betydande kostnadsökningar och praktiska svårigheter i det dagliga arbetet. Det kan nämnas att datainspektionen har möjligheter att ge föreskrifter om kryptering och om behörighetssystem i den mån det anses erforderligt som skydd för den personliga integriteten.

När det gäller behörighetssystem har leverantörerna på senare tid lagt ner mycket möda på att utveckla sådana. I dag kan en del leverantörer erbjuda en hel del säkerhetsanordningar inbyggda i maskin- och programvara. I maskinvaran kan t ex spärrar vara inbyggda som gör det möjligt att begränsa behörigheten att utföra olika arbetsuppgifter. I programvaran kan finnas användarlistor som anger vilka olika projekt och tillämpningar olika användare får gå in i och vilka data de har tillgång till samt spärrar som hindrar överskridanden.

Enligt SÅRKs mening kan användning av kryptering och behörighetssystem — liksom andra säkerhetsåtgärder — givetvis bidra till att minska sårbarheten vad gäller nu diskuterade register. Emellertid får man hålla i minnet att dessa hjälpmedel ingalunda ger ett komplett skydd. Vidare kan användningen medföra ökade kostnader och praktiska svårigheter. En ökad användning av kryptering får dock anses som något angeläget. Genom att krypteringsmetoderna undan för undan förbättras underlättas även sådan användning. När det gäller kryptering torde förbindelsekryptering[1] vara den som idag är den som är mest praktiskt användbar och i många situationer gör naturligtvis sådan kryptering stor nytta. Å andra sidan är det ofta svårt för obehöriga att få tag på den information de är intresserade av medan denna är under transport. Ofta är det endast en bråkdel av den totala informationen som sänds iväg vilket redan det har en begränsande effekt. Vidare måste det ofta vara en ren lyckträff om den som obehörigen avlyssnar kommunikationerna kommer över information som han kan använda. Den som är intresserad av att obehörigen skaffa information torde därför som regel ha betydligt mer att hämta på det ställe där informationen finns lagrad. Detta innebär att registerkryptering[2] i flertalet fall kan vara av större värde än förbindelsekryptering. Det ena utesluter för övrigt inte det andra. Registerkryptering kan naturligtvis vara både dyrbar och medföra besvär vid den dagliga hanteringen av information. Det måste närmast bli en bedömning från fall till fall i vad mån och i vilken omfattning kryptering och olika behörighetsystem bör komma till användning. Man får då även vara beredd att godta en del extra kostnader och besvär.

6.3 Möjligheten att sprida datorkraft

I avsnittet om koncentration har SÅRK uttalat att det är av stort intresse att notera att den tekniska utvecklingen fortsätter i sådan riktning att en spridning av datorkraften underlättas. Några remissinstanser, bland andra en av de större leverantörerna, påpekar att utvecklingen därvidlag t o m går snabbare än vad kommittén synes anta.

Framförallt går utvecklingen oerhört snabbt såtillvida att datorerna blir allt mindre, snabbare och billigare. Detta innebär även att datorerna kan användas inom många nya områden och på annat sätt än tidigare. Det innebär framförallt att pris och teknik medger att varje användare, det kan gälla myndighet eller annan, kan skaffa sig datorer och system

[1] Kryptering av information som skall överföras genom datakommunikation

[2] Kryptering av information som ligger lagrad på ADB-medium

som passar just honom. I detta sammanhang kan nämnas att en leverantör har framställt mikrodatorer som byggts in i ett plastkort. Detta har ungefär samma storlek och form som ett vanligt kreditkort och kan alltså lätt förvaras i fickan eller i en plånbok. Datorn har både lagrings- och bearbetningsmöjligheter. Kortet kan laddas med information om t ex banktillgodohavanden. Med speciell apparatur kan kortet läsas av och en bearbetning göras som möjliggör en betalningsöverföring och att ny kontoställning läggs in på kortet. Kortet med datorn är tänkt som en förbrukningsartikel, bl a för att hindra missbruk. Man kan göra så att kortet blir obrukbart när det tömts på sin ursprungsinformation t ex i form av det grundbelopp som matats in. Tillämpningar av nu diskuterat slag kan naturligtvis ha positiva effekter från sårbarhetssynpunkt. Emellertid kan nya sådana tillämpningar enligt SÅRKs mening, även vålla nya sårbarhetsproblem. Även om man söker lösa olika säkerhetsproblem kan man aldrig gardera sig helt mot missbruk av olika slag. Tillämpningarna kan exempelvis ställa nya krav på grundregistren.

6.4 Utlandsberoende

Vad gäller utlandsberoendet har en del remissinstanser erinrat om att det finns ett utlandsberoende även vad gäller programvara och behörighetssystem, något som inte berörts i lägesrapporten. SÅRK delar remissinstansernas uppfattning i denna fråga. Särskilt känsligt kan sådant beroende bli för användare som helt förlitar sig på utländska programvaruhus. Å andra sidan bör framhållas att de negativa effekterna av nu diskuterat utlandsberoende ofta kan begränsas. Vid t ex en avspärrningssituation kan detta ske genom att systemen används utan att några ändringar införs i dem.

SÅRK har, av en del remissinstanser, fått stöd i sin uppfattning att det i vissa fall kan finnas skäl att granska bearbetningar som sker utomlands. Ett exempel anförs av LMV som i sitt yttrande menar att vissa bearbetningar av tekniska data inte bör få utföras utomlands utan särskilt tillstånd. För lantmäteriets del gäller detta från underrättelsesynpunkt känslig landskapsinformation.

6.5 Standardisering

Vid remissbehandlingen har framkommit synpunkter på vilken betydelse standardisering kan ha för en i olika avseenden minskad sårbarhet. Standardisering och tillämpningen av standarder i olika ADB-system — det kan gälla datorer, program, dokumentation, datakommunikationsutrustning etc — ger ökad kompatibilitet. Detta innebär bl a ökade möjligheter att utan särskild konvertering överflytta ett program eller ett helt system från en datoranläggning till en annan. En annan form av kompatibilitet består i att den ger möjlighet att byta ut eller kombinera olika utrustningsenheter vid en datoranläggning. Ge-

nom kompatibiliteten ges bättre förutsättningar för att olika anläggningar skall kunna fungera som reservanläggningar för varandra.

Standardisering gör det även lättare att flytta personal mellan olika system, ger bättre reservdelsmöjligheter och tillgång till underhållspersonal. Genom ökad standardisering kan man alltså minska personalberoendet, minska utlandsberoendet och få bättre back-upmöjligheter.

Staten bidrar med medel till olika standardiseringsprojekt inom ADB-området. Bl a beviljas särskilda medel till Sveriges standardiseringskommission (SIS) för standardisering inom ADB-sektorn. Sedan 1974 finns ett standardiseringsråd knutet till statskontoret. Rådets uppgift är att verka för ökad samordning inom den offentliga sektorn vad gäller teknisk standardisering inom ADB-området. Rådet skall även verka för en samordning av den offentliga sektorns insatser i det nationella och internationella standardiseringsarbetet inom ADB-sektorn.

Enligt SÅRKs mening är det väsentligt att ett fortlöpande arbete sker på standardiseringsområdet — och att standardiseringsproblemen uppmärksammas i samband med upphandling. Det ligger emellertid stora svårigheter i att få olika leverantörer att ena sig om gemensamma standarder beträffande maskin- och programvara.

När det gäller standardisering av dokumentation är uppgiften måhända något lättare. I vart fall när det gäller den offentliga sektorn borde en ökad standardisering kunna ske beträffande dokumentation och även kryptering.

Något som kan bidra till en förbättrad situation på standardiseringsområdet är den ökade användningen av datakommunikationer med ökande användning även av dator till datorförbindelser. För att samverkan på olika sätt skall kunna äga rum med hjälp av datakommunikationer ställs även krav på kompatibilitet och detta bör medföra att många användare kommer att fästa större vikt vid standardiseringsfrågor och i framtiden även ställa större krav på leverantörerna när det gäller standard.

7 Kompetensfördelningen inom regeringskansliet och mellan olika statliga myndigheter vad gäller ADB-frågor m m

7.1 Allmänt

I departementsförordningen (1963:214) finns bestämmelser om vilka förvaltningsärenden och vilka lagstiftningsområden som hör till de olika departementen. Vad gäller användningen av ADB finns inte något övergripande ansvar hos visst departement. Grundprincipen är den — liksom på myndighetsnivå — att ADB ses som ett hjälpmedel för olika verksamheter. Ansvaret för ADB-hanteringen knyts därmed i första hand till den som har ansvaret för den verksamhet i vilken ADB kommer till användning.

År 1977 inrättades en särskild samrådsgrupp för datafrågor inom regeringskansliet med uppgift att vara ett rådgivande och samordnande organ.

I samband med budgetarbetet sker även en granskning av myndigheternas ADB-användning. På senare tid har även större krav ställts på anslagsframställningarnas innehåll när det gäller ADB-användning. Härigenom har möjligheterna ökat att styra den statliga ADB-användningen.

I propositionen 1978/79:121 om användning av ADB i statsförvaltningen, som i stort godtagits av riksdagen, föreslås bl a en starkare styrning från statsmakternas sida vad gäller den statliga ADB-användningen. Vid behandlingen av propositionen beslutade riksdagen även att en datadelegation knuten till regeringskansliet skulle inrättas.

De nu berörda samordningsfrågorna behandlas utförligare i avsnitt 8.1 nedan.

I det följande kommer olika myndigheter och affärsdrivande verk att beskrivas departementsvis.

7.2 Justitiedepartementets område

Justitiedepartementet

Departementet har ansvar för datalagstiftningen och bereder besvärsärenden enligt datalagen. Vidare ansvarar departementet för lagstiftning som rör offentlighet, sekretess och tystnadsplikt.

Inom justitiedepartementets område sker en central samordning av myndigheternas användning av ADB, framförallt systemutveckling. I RI-kungörelsen (1970:517) regleras samarbetet mellan de myndigheter som medverkar i s k RI-projekt (RI = rättsväsendets informationssystem). Samarbetsorganet för rättsväsendets informationssystem (SARI) har ett övergripande ansvar för beredning av ADB-frågor inom RI.

I regleringsbrev till myndigheterna anges hur stora resurser som får användas för datorbearbetningar och för vilka system och ändamål resurserna får användas. Förslag till nya ADB-rutiner eller väsentligt ändrade ADB-rutiner som inte skall ingå i RI skall underställas regeringen. Förslag till ändringar inom RI underställs SARI.

Rikspolisstyrelsen (RPS)

Enligt sin instruktion (1965:674) skall RPS bl a leda den särskilda polisverksamheten för att hindra och uppdaga brott mot rikets säkerhet m m. I kungörelsen (1966:273) om säkerhetsskydd vid statsmyndighet sägs i 1 § att statsmyndighet som har befattning med uppgift eller förhållande som angår rikets försvar eller landets säkerhet i övrigt skall vidta åtgärder för säkerhetsskydd inom sitt verksamhetsområde. I 2 § beskrivs närmare vad säkerhetsskydd innefattar. Enligt 4 § skall allmänna föreskrifter om tillämpningen av kungörelsen meddelas av ÖB för de flesta myndigheter som hör till försvarsdepartementet medan RPS har motsvarande funktion för övriga myndigheter. RPS skall på anfordran lämna riksdagen och dess verk råd och anvisningar om säkerhetsskydd. Råd och anvisningar om teknisk skyddsåtgärd lämnas av RPS till alla myndigheter. Allmänna föreskrifter om tillämpning av säkerhetsskyddskungörelsen, AFSÄK, har fastställts och utgivits av RPS och ÖB den 1 juni 1970. AFSÄK är för närvarande under omarbetning. I AFSÄK 1970 finns även ett avsnitt om säkerhet vid ADB-behandling.

Datainspektionen (DI)

Enligt sin instruktion (1973:292) har DI som central förvaltningsmyndighet till uppgift att pröva frågor om tillstånd och att utöva tillsyn enligt bl a datalagen (1973:289) och kreditupplysningslagen (1973:1173).

I datalagen finns bestämmelser — vad gäller personregister förda med hjälp av ADB — som skall bidra till att skydda den personliga integriteten. Personregister får inte inrättas och föras utan tillstånd av DI. Detta gäller såväl den offentliga som privata sektorn. I de fall statsmakterna beslutar om inrättande av personregister måste DI först höras.

I 3 § och 3 a § datalagen finns bestämmelser som bl a tar sikte på befolkningsregister och i 4 § bestämmelser om register med särskilt känslig information. Enligt 5 § har DI rätt att ge föreskrifter om ändamål med och innehåll i personregister. I 6 § ges möjlighet till föreskrifter av annat slag bl a om dokumentation, lagring, gallring, säkerhet m m. I 11 § finns regler som tar sikte på dataflödet av personuppgifter över gränserna. För att även register inom den offentliga sektorn skall omfattas av sådana

regler har motsvarande bestämmelser införts i sekretesslagen. 21 § innehåller bestämmelser om dataintrång och gäller alla sorts register alltså även register som inte innehåller personuppgifter.

DI skall genom tillsynsverksamhet se till att datalagens regler efterföljs.

DI är även tillstånds- och tillsynsmyndighet vad gäller ärenden enligt kreditupplysningslagen. Denna lag reglerar såväl manuella register som ADB-register som förs i kreditupplysningsverksamhet. Lagen omfattar även registrering av juridiska personer.

Enligt instruktionen för DI åligger det inspektionen särskilt att med uppmärksamhet bl a följa utvecklingen i fråga om automatisk databehandling av personuppgifter och inom sitt verksamhetsområde lämna myndigheter, organisationer och enskilda, råd och upplysningar.

7.3 Försvarsdepartementets område

Försvarsdepartementet

Departementet har ansvaret för större delen av totalförsvaret och svarar även för samordningen av detta. Departementets sekretariat för säkerhetspolitik och långsiktsplanering inom totalförsvaret (SSLP) har bl a ägnat samhällets sårbarhet stort intresse och även presenterat ett antal rapporter inom detta område bl a gäller detta områdena datoranvändning och telekommunikationer.

Den datakraftplan som utarbetats av ÖB bygger på ett regeringsbeslut från år 1975. Olika projekt inom försvarsdepartementets område prövas kontinuerligt av regeringen vid olika kontrollstationer då det avgörs om fortsatt utveckling skall ske.

Överbefälhavaren (ÖB)

ÖB har enligt sin instruktion (1968:408) under regeringen ledningen av och uppsikten över försvarsmakten. Till ÖBs uppgifter hör att leda underrättelse- och säkerhetstjänsten inom försvarsmakten.

Vidare skall ÖB verka för enhetlighet inom försvarsmakten och främja samverkan mellan försvarsmakten och övriga myndigheter och institutioner inom totalförsvaret.

För att tillgodose det behov som finns av planering och samordning vid utveckling av informationssystem samt anskaffning och utnyttjande av ADB-utrustning för försvarsmakten har ÖB utarbetat en informationssystem- och datakraftplan. I planen har ÖB satt upp mål för utbyggnad av försvarets datakraft under den närmaste tioårsperioden.

Enligt 4 § i kungörelsen om säkerhetsskydd vid statsmyndigheter skall allmänna föreskrifter om tillämpning av kungörelsen meddelas av ÖB för myndigheter som hör till försvarsdepartementet med undantag av civilförsvarsstyrelsen och beredskapsnämnden för psykologiskt försvar. Kontroll av säkerhetsskydd vid dessa myndigheter utförs av ÖB. Myn-

dighet som behöver biträde med sitt säkerhetsskydd skall vända sig till den myndighet som meddelar råd och anvisningar. ÖB är tillsammans med RPS skyldig att på begäran lämna riksdagen och dess verk råd och anvisningar om säkerhetsskydd.

Försvarets datacentral

Datacentralen har enligt sin instruktion (1974:612) till uppgift att med datorutrustning som ställs till förfogande på uppdrag utföra främst administrativ databehandling åt myndigheter som hör till försvarsdepartementet. Datacentralen skall vidare svara för beredskaps- och krigsplanläggning i fråga om driften av den datorutrustning som ställs till datacentralens förfogande.

Datacentralen skall följa de direktiv med allmänna riktlinjer för datacentralens verksamhet och de anvisningar rörande verksamhetens närmare utformning som ÖB meddelar för att tillgodose den operativa verksamhet och långsiktsplaneringen inom krigsmakten.

Försvarets rationaliseringsinstitut (FRI)

FRI är enligt sin instruktion (1968:340) central förvaltningsmyndighet för rationaliseringsverksamhet inom den del av statsförvaltningen som hör till försvarsdepartementet. Det åligger FRI särskilt att, bl a gentemot statskontoret, svara för samordning i fråga om anskaffning och utnyttjande av datorer. Som en del av rationaliseringsverksamheten ingår även att medverka i systemutvecklingsarbete.

7.4 Kommunikationsdepartementets område

Kommunikationsdepartementet

Detta departement har ett övergripande ansvar för datakommunikationsfrågor.

Televerket

Enligt sin instruktion (1965:842) skall televerket svara för anläggning, drift och förvaltning av de statliga teleanläggningar som är underställda verket. Televerket skall vidare se till att samhällets och enskildas behov av telekommunikationer tillgodoses. Verksamheten i fred skall bedrivas så att även de krav som det totala försvaret i krig uppställer i största möjliga utsträckning kan tillgodoses. Televerket skall samråda med ÖB och andra totalförsvarsmyndigheter. Det kan även nämnas att televerket deltar i ett omfattande internationellt samarbete på telekommunikationsområdet.

Dataöverföring har hittills skett via telenätet och sådan överföring har under senare år expanderat kraftigt. År 1976 fattade riksdagen beslut om

att inrätta ett allmänt datanät. Nätet tas i drift vid årsskiftet 1979/80 och byggs ut i nära samarbete med övriga nordiska länder.

Det bör även nämnas att televerket genom sin verksamhet med att tillhandahålla datakommunikationstjänster har ett starkt intresse för standardiseringsfrågor när det gäller datatrafiken.

7.5 Budgetdepartementets område

Budgetdepartementet

Departementet har en central ställning vad gäller ADB-frågor. Detta beror bl a på budgetregleringsfunktionen. Departementet har vidare ett allmänt ansvar för rationaliserings- och upphandlingsfrågor samt för förvaltningsrevision.

Statskontoret

Statskontoret är enligt sin instruktion (1965:703) central myndighet för rationaliseringsverksamheten inom statsförvaltningen i den mån denna uppgift inte ankommer på annan myndighet. Statskontoret skall även svara för samordning ifråga om anskaffning och utnyttjande av datorer inom statsförvaltningen. Enligt 3 § rationaliseringsförordningen (1975:567) bör myndighet vid utveckling av ADB-system och annan rationaliseringsverksamhet så tidigt som möjligt samråda med statskontoret i frågor som är av större omfattning eller av principiell betydelse.

Statskontoret medverkar ofta i samband med utvecklande och införande av ADB-system (systemutvecklingsarbete m m). Detta sker i huvudsak på grundval av myndighetens övergripande rationaliseringsansvar.

Anskaffningen av generellt användbar ADB-utrustning i statsförvaltningen med undantag för affärsverken sker centralt genom statskontoret som även i övrigt svarar för samordning i fråga om användning av ADB i statsförvaltningen. Genom begränsningen till generella datorer faller specialtillverkad utrustning som förekommer — t ex inom försvaret — utanför statskontorets upphandling. Vidare gäller upphandlingen i huvudsak själva maskinvaran. Beslut om införande av ADB som hjälpmedel är i regel något som ankommer på myndigheterna själva. Utgifterna för utrustningen finansieras med medel från en särskild kapitalfond, datamaskinfonden. Fonden kommer att upphöra och ersättas med någon form av investeringsanslag.

Frågor som rör samordnad anskaffning av utrustning för ADB i statsförvaltningen utreds för närvarande.

Vad gäller ADB-säkerhetsarbetet har detta bedrivits som ett projekt som organisatoriskt hörde till DASKs utredningsarbete. Projektet leds av statskontoret. Arbetet delades upp i fyra delprojekt; kapitalskydd, funktionsskydd, dataskydd och kvalitetsskydd. Säkerhetsarbetet har resulterat i ett flertal rapporter.

Det skall slutligen nämnas att statskontoret nyligen varit föremål för utredning vad gäller framtida organisation, uppgifter, verksamhet m m. Resultatet är redovisat i betänkandet Rationalisering och ADB i statsförvaltningen (SOU 1979:72).

DAFA

DAFA har enligt sin instruktion (1975:570) till uppgift att på uppdrag av statliga organ utföra administrativ databehandling och arbeta med metod- och systemutveckling i samband med sådana uppdrag. Det gäller i första hand civila myndigheter. Det åligger DAFA särskilt att bl a utfärda anvisningar och rekommendationer av betydelse för de ADB-system vilkas drift förläggs till DAFA och att tillhandahålla generella ADB-program för sådana ADB-tillämpningar som ofta förekommer hos myndigheterna.

Enligt rationaliseringsförordningen bör myndighet till DAFA lämna sådana uppdrag som avser anpassning av standardystem som DAFA tillhandhåller. Myndighet skall vid införande eller förändring av ADB-rutiner i första hand använda de färdiga program för ADB-system som DAFA eller annan myndighet kan tillhandahålla om de är lämpliga för avsett ändamål.

Den s k monopolutredningen har föreslagit att DAFAs särställning i bl a dessa avseenden upphävs. Detta förslag redovisas närmare under 8.1.3 nedan.

Riksrevisionsverket (RRV)

RRV skall enligt sin instruktion (1977:444) utgöra central förvaltningsmyndighet för revision och redovisning samt därmed sammanhängande frågor inom statsförvaltningen. Det åligger verket särskilt att bl a granska den statliga verksamheten och tillse att den bedrivs effektivt, granska hur den statliga upphandlingen bedrivs och verka för samordningen av denna samt följa myndigheternas tillämpning av kungörelsen (1970:641) om begränsning i myndighets rätt att meddela föreskrifter, anvisningar och råd.

Som revisionsmyndighet har RRV även möjlighet att granska ADB-verksamhet i löpande drift. Medverkan i systemutvecklingsarbete anses däremot i första hand vara en uppgift för rationaliseringsorganen likom utformning av normer och standarder för hur sådant arbete skall bedrivas (se budgetproposition 1976/77 bilaga 11 sid 50 f).

7.6 Handelsdepartementets område

Handelsdepartementet

Departementet har det övergripande ansvaret för det ekonomiska försvaret.

Överstyrelsen för ekonomiskt försvar (ÖEF)

ÖEF är enligt sin instruktion (1978:291) central förvaltningsmyndighet för det ekonomiska försvaret. Inom ramen för sitt samordningsansvar inom detta område skall ÖEF bl a utforma allmänna riktlinjer för beredskapsåtgärder inom det ekonomiska försvaret och vid behov föreslå andra myndigheter sådana åtgärder.

Myndigheten skall skaffa sig kännedom om bl a landets näringsliv; landets förbrukning av och tillgångar på energi, råvaror och andra förnödenheter; landets export och import.

I den mån det inte ankommer på annan myndighet skall ÖEF vidta förberedelser så att landets behov av förnödenheter och tjänster, som är av vikt för totalförsvaret eller folkförsörjning, skall kunna tillgodoses vid krig eller krigsfara eller under andra utomordentliga förhållanden. ÖEF skall därvid särskilt förbereda åtgärder för att möta försörjningssvårigheter vid s k fredskriser. Styrelsen har alltså det direkta ansvaret för planläggning inom områden som inte kan hänföras till någon annan myndighets fredstida verksamhet. Hit hör bl a huvuddelen av industriproduktionen och handeln. ÖEF har ansvaret för beredskapsplaneringen av flertalet förnödenheter. (För livsmedel och fodermedel har jordbruksnämnden motsvarande funktion som ÖEF för andra förnödenheter.)

ÖEF för med stöd av lagen (1948:390) om skyldighet för näringsidkare m fl att biträda vid planläggningen av rikets ekonomiska försvarsberedskap, ett register över krigsviktiga företag, s k K-företag.

ÖEF har vissa centrala funktioner som rör lagen (1961:655) om undanförsel och förstöring med följdförfattningar. Överstyrelsen har även utfärdat närmare anvisningar för undanförsel och förstörning, något som åligger myndigheten enligt kungörelsen (1961: 656) om undanförsel och förstöring.

I detta sammanhang kan nämnas att i förordningen (1977:55) om vissa statliga myndigheter beredskap m m finns bestämmelser (39 och 44 §§) om vad myndigheter som ej ingår i försvarsmakten har att iaktta vad gäller bl a databehandlad information och personregister av större omfattning i ett beredskapsläge (beredskapsgrad II). Motsvarande bestämmelser finns även för beredskapsgrad I (högsta beredskapsgraden).

I Kungl Maj:ts föreskrifter den 27 september 1974 finns bestämmelser om statliga myndigheters planläggning av informationsbehandling i krig i sådana fall då automatisk databehandling används i fred och kan ifrågakomma i krig (jfr 4.3.3 ovan). ÖEF har enligt dessa föreskrifter ålagts att samordna och meddela erforderliga anvisningar för beredskapsplaneringen inom totalförsvaret vad gäller sådan informationsbehandling som kräver datorstöd. Samordningen av planeringen mellan försvarsmaktens myndigheter ligger dock utanför ÖEFs ansvarsområde.

7.7 Industridepartementets område

Industridepartementet

Departementet handlägger bl a ärenden som rör näringspolitiken och som rör teknisk forskning och utvecklingsarbete.

Industriverket (SIND)

Verket är enligt sin instruktion (1974:476) central förvaltningsmyndighet för ärenden som bl a rör industri, och hantverk och energiförsörjning. Det åligger verket särskilt, att bl a främja näringslivets tekniska och ekonomiska utveckling med särskild hänsyn till mindre och medelstora företag och att göra utredningar i frågor som rör industriområdet samt att planera och samordna statliga industripolitiska stöd och utvecklingsinsatser i den mån detta inte ankommer på annan myndighet. I budgetpropositionen 1975 gav regeringen SIND i uppdrag att inom sitt område fortlöpande bevaka utvecklingen inom datorområdet.

Styrelsen för teknisk utveckling (STU)

STU är enligt sin instruktion (1968:404) central förvaltningsmyndighet för initiativ och stöd till samt planläggning och rådgivning rörande teknisk forskning och industriellt utvecklingsarbete i den mån sådana uppgifter inte ankommer på annan statlig myndighet. STU stödjer även utvecklingen på det datatekniska området.

7.8 Kommundepartementets område

Kommundepartementet

Inom departementet övervägs bl a frågor som sammanhänger med ADB som hjälpmedel vid samhällsplanering. Till departementet hör även ADB-beredningsgruppen (C 1973:06) som är tillsatt för att behandla frågor om utveckling och utnyttjande av ADB med anknytning till samhällsplanering inom länsstyrelserna m m.

Länsstyrelserna

Länsstyrelserna har viktiga funktioner vad gäller samhällsplanering.

Vidare har länsstyrelserna vissa uppgifter vad gäller planläggningen av totalförsvaret. Bl a ankommer det på länsstyrelsen att inom varje län planlägga undanförsel och förstöring i enlighet med de anvisningar som ÖEF meddelar i samråd med berörda myndigheter.

7.9 Övrigt

Ytterligare några myndighetsfunktioner av intresse skall i korthet beröras. Sålunda bör nämnas att värnpliktsverket och arbetsmarknadsverket fyller vissa centrala funktioner vad gäller uppskovsförfarandet enligt uppskovskungörelsen (1973:939). Vidare skall nämnas att UHÄ och SÖ har det övergripande ansvaret för ADB-utbildningen vid allmänna läroanstalter och att ADB-utbildning av ganska omfattande karaktär drivs av bl a SIPU.

När det gäller standardiseringsfrågor finns sedan 1974 ett råd knutet till statskontoret — *statskontorets standardieringsråd* — för samråd i frågor om det tekniska standardiseringsarbetet på ADB-området inom den offentliga sektorn.

Sveriges standardiseringskommission (SIS) är centralorgan för den nationella standardiseringsverksamheten och företräder Sverige i det internationella standardiseringsarbetet. SIS verksamhet finansieras bl a genom statsbidrag.

8 Pågående datapolitisk utveckling

Den nya tekniken och den tekniska utvecklingen har under 1970-talet föranlett ett antal utredningar av såväl frågor om användningen av ADB inom olika verksamhetsområden som ADB-frågor av mer principiell och övergripande karaktär. Vidare har flera utredningar nyligen tillsatts för att närmare studera datateknikens effekter och utvecklingsmöjligheter på skilda samhällsområden. Nedan redogörs huvudsakligen för den datapolitiska utvecklingen efter det att SÅRK angav sin lägesrapport och i de delar som har direkt betydelse för eller väsentliga beröringspunkter med sårbarhetsproblemen.

8.1 Samordningsfrågor

År 1977 inrättade regeringen samrådsgruppen för datafrågor med uppgift att vara ett samrådsorgan inom regeringskansliet för beredning av viktigare datafrågor innefattande dels frågor av policykaraktär och dels frågor rörande enskilda dataprojekt m m. Budgetministern var gruppens ordförande. Ledamöter i gruppen var företrädare för de tre regeringspartierna. I samband med regeringsskiftet hösten 1978 ändrades gruppens sammansättning. Ordförande för gruppen var därefter statssekreteraren i budgetdepartementet. Gruppens ledamöter var statssekreterarna i statsrådsberedningen, justitie-, försvars-, kommunikations-, arbetsmarknads-, industri- och kommundepartementen. Gruppen har fungerat som samrådsorgan dels för vissa mer avgränsade ADB-frågor och dels för arbetet med princippropositionen 1978/79:121 om användningen av ADB i statsförvaltningen.

8.1.1 *Datapolitisk principproposition*

Datasamordningskommitteen som hade till huvuduppgift att belysa möjlig och önskvärd samordning på ADB-området avgav slutbetänkandet ADB och samordning (SOU 1976:58). Betänkandet utgör tillsammans med visst annat utredningsmaterial underlag för de överväganden och ställningstaganden som redovisas i princippropositionen 1978/79:121 om användningen av ADB i statsförvaltningen. I propositionen framhölls att den endast gav uttryck för en del av regeringens samlade

datapolitik och att flera utredningar tillsatts för att studera olika ADB-frågor och effekterna av datatekniken.

I propositionen föreslogs att statsmakterna skall ges tillfälle att ta ställning till ADB-systemens ändamål, ambitionsnivån i datorstödet, system- och driftstrukturerna samt i vilken takt ADB skall införas på olika områden.

De ändamål för vilka ADB används i administrativ verksamhet och de förbättringar som därvid eftersträvas sammanfattades sålunda: lägre kostnader och mindre resursuppoffringar, bättre information och beslutsunderlag, snabbare ärendehandläggning, bättre uppföljning och kontroll, bättre arbetsförhållanden, bättre prestationer och service samt nya organisations- och arbetsformer. Viktiga faktorer som påverkar hur ADB bör få användas och hur ADB-funktioner bör organiseras angavs vara samhällets och förvaltningens sårbarhet, rättssäkerhet och integritetsskydd, arbetsförhållanden och sysselsättning, medbestämmande för personalen, decentralisering samt insyn i förvaltningen.

Sammanfattningsvis föreslogs följande åtgärder:

1. Formella regler utfärdas för etappindelning, beslutspunkter och beslutsunderlag i samband med systeminvesteringar. Fasta beslutspunkter införs för att bl a säkerställa att ansvariga instanser och personer kommer in i processen i tillräcklig utsträckning. Reglerna för beslut rörande större och viktigare investeringar samlas i en särskild handläggningsordning.

2. Planering och administration av ADB-drift förbättras. Större datacentraler åläggs att utarbeta årliga verksamhetsberättelser.

3. Myndigheternas redovisning ordnas så att kostnaderna för ADB kan urskiljas och ADB särredovisas i myndigheternas anslagsframställningar.

4. Myndigheternas planering av ADB-användningen förbättras och de åläggs att i anslutning till anslagsframställningarna redovisa pågående och planerad utveckling och drift av ADB-system.

5. Anvisningar om hur ADB bör administreras inom myndigheterna utfärdas.

Handläggningsordningen föreslås gälla större eller viktigare projekt och bör finnas i ett särskilt dokument. Av handläggningsordningen skall framgå det ansvar som åvilar regeringen, de centrala rationaliseringsorganen och myndigheter. Handläggningsordningen innebär alltså att man för större projekt inte skall vara bunden till den ordinarie budgetprocessen. Preliminära beräkningar av medelsbehovet bör dock göras i anslagsframställningarna. Medlen skall ställas till förfogande efter beslut om fortsatt arbete. Utveckling eller större ändringar av ADB-system bör delas in i etapper; initiering, förstudie, huvudstudie, systemkonstruktion, drift och förvaltning samt efterstudie. Övergång från en etapp till en annan bör föregås av beslut av ansvarig instans. Regeringen bör

granska förstudien och huvudstudien samt ges tillfälle att innan systemet tas i drift kontrollera hur systemet uppfyller ställda krav och att det får rimliga effekter i övrigt.

Lämplig tidpunkt för sistnämnda beslutspunkt bör avgöras för varje projekt. De systeminvesteringar som följer den särskilda handläggningsordningen förutsätts på lämpligt sätt anmälas för riksdagen i samband med för- eller huvudstudien samt i övrigt om förutsättningarna väsentligt förändras.

I handläggningsordningen avses omfattningen och formerna för de centrala rationaliseringsorganens medverkan att preciseras. Vilka projekt som skall omfattas av den föreslagna handläggningsordningen kommer att övervägas i arbetet med att utforma denna.

Mindre projekt bör också följa reglerna i handläggningsordningen, men myndigheterna skall själva ha ansvaret för att dessa system blir lämpliga. Dessa mindre projekt liksom underhållsarbete och ADB-drift bör behandlas i den ordinarie budgetprocessen.

En samlad presentation av myndigheternas ADB-användning bör alltid ges. I anslagsframställningarna bör därför lämnas en kort redogörelse för vilka system som är i drift eller under utveckling. Även de projekt som följer den särskilda handläggningsordningen bör redovisas i detta sammanhang. Arbete pågår med att utforma vägledning för myndigheternas utformning av anslagsframställningarna.

Behov anses föreligga av ADB-planer innefattande en samlad och översiktlig redogörelse för i princip alla vid en myndighet aktuella ADB-projekt. Formerna härför avses prövas närmare.

Anvisningar föreslås för hur utvecklingsarbete och datordrift i stort bör bedrivas vid myndigheter. Anvisningarna bör ange hur uppgifts- och ansvarsfördelningen normalt bör fördelas mellan verksledning, ADB-funktion, driftenheter och sakenheter. Vidare bör anges vilka rapporteringsrutiner och planeringsdokument som alltid bör finnas.

Systemutvecklingen bör ske gemensamt för statliga verksamheter som förekommer i hela landet och som är eller bör vara enhetliga. Detta innebär emellertid inte att alla regionala eller lokala enheter skall ha samma datorstöd. Ansvaret för utveckling av ADB-system bör alltid läggas på den för respektive verksamhet ansvariga myndigheten. Större ADB-användare bör i regel ha egen personal för utveckling och underhåll av ADB-system. Det konstateras att systemutvecklingsresurserna f n i hög grad är koncentrerade till Stockholmsområdet. Regionalpolitiska och andra skäl anses tala för en spridning t ex genom lokalisering av utvecklingsenheter eller delar av utvecklingsenheter till andra orter.

Beträffande datordriften anges två huvudprinciper. Den ena principen är att datordrift som är av större omfattning skall ske för varje verksamhet för sig (s k dedicerad eller myndighetsspecifik drift). För detta talar bl a kraven på tillgänglighet, säkerhet, förändringsbarhet och användarnas möjligheter att påverka systemens utformning och prestationer.

Den andra principen är att datordriften inom en verksamhet på lämpligt sätt bör spridas. Driftlösningar som bygger på spridning har fördelar

bl a vad avser säkerhet och sårbarhet. Hur datordriften bör spridas i varje enskilt fall är en avvägningsfråga. Faktorer som bör påverka den närmare utformningen är, förutom säkerhetsaspekter, den datorstödda verksamhetens organisation, databehandlingens omfattning och karaktär samt de beräknade kostnaderna.

Det framhålls i sammanhanget att det av ekonomiska skäl är angeläget att gjorda investeringar får ett rimligt utnyttjande. Därför bör spridningen i vad avser befintliga system ske med noggrann planering och i en väl avvägd takt.

Servicebyråer anses behövas även i framtiden och kan vara ett alternativ för myndigheter som använder ADB i liten utsträckning, vid försöksverksamhet eller för tillhandahållande av tjänster som kräver tillgång till speciell utrustning.

Vidare anses att den samordnade anskaffningen av ADB-utrustning som har flera fördelar för såväl myndigheter som för staten bör behållas.

Åtgärder aviseras för att förbättra metodstödet, informations-och erfarenhetsförmedlingen m m för utveckling och drift av ADB-system.

Ett sätt att ge särskilt riksdagen bättre översiktlig information i samlad form anges vara att ta in ett speciellt avsnitt om ADB i bilaga till budgetpropositionen.

Avslutningsvis behandlades i propositionen frågan om inrättande av ett dataråd e d för principiella och övergripande frågor. Ett organ av sådan typ angavs kunna fylla en viktig funktion. Eftersom en rad av de frågor som skulle behandlas i ett sådant råd — bl a frågorna om sårbarhet, sysselsättning och arbetsmiljö samt datateknikens effekter på näringslivets utveckling — f n utreds ansågs det dock inte vara rätt tidpunkt att inrätta ett sådant organ. Vidare angavs frågan påverkas av utredningen (B 1979:01) av organisationen för de centrala myndighetsuppgifterna avseende rationalisering och ADB. Tanken på ett dataråd borde därför prövas på nytt i samband med att resultat av pågående utredningar kommer fram.

8.1.2 *Riksdagens ställningstagande till den datapolitiska princippropositionen*

Finansutskottet redovisade i betänkande (FiU 1978/79:34) bl a följande synpunkter. Utskottet betonade att dess behandling av propositionen avsåg de stora dragen och skedde från principiella utgångspunkter. Särskilt framhöll utskottet nödvändigheten av att förbättra statsmakternas insyn i användningen av ADB och av att ge statsmakterna bättre möjligheter att påverka inriktningen av ADB-användningen samt att detta bl a kräver att ett lämpligt utformat beslutsunderlag tas fram vid olika tillfällen. I normalfallet bör riksdagens ställningstagande följa när resultatet av en s k huvudstudie föreligger men innan systemkonstruktion påbörjas. Vid väsentligt förändrade förutsättningar bör dock ärendet på nytt underställas riksdagen. Med hänsyn till utredningen om den centrala myndighetsorganisationen avseende rationaliering och ADB borde man enligt utskottets mening inte nu binda sig för den närmare

utformningen av granskningsfunktionen. Utskottet underströk emellertid vikten av att en effektiv granskning sker.

Beträffande systemutveckling och datordriftens organisation anslöt sig utskottet till huvudprinciperna i propositionen om att ansvaret för ADB-verksamheten normalt bör ligga hos den myndighet som ansvarar för verksamheten i övrigt. För datordriften bör enligt utskottets mening eftersträvas att driften blir specifik för myndigheten (dedicerad) och att en spridning av driftställen eftersträvas inte minst i syfte att minska sårbarheten. Utskottet pekade också bl a på utbildningens roll och att det i första hand bör ankomma på statens rationaliserings- och utbildningsmyndigheter att planera denna.

Beträffande frågan om inrättande av ett dataråd eller datadelegation fann utskottet vid sin beredning av frågan starka skäl tala för att en datadelegation knuten till regeringskansliet inrättas. En huvuduppgift för datadelegationen bör enligt utskottet vara att bevaka utvecklingen av datoriseringen, främja kunskapsutvecklingen på området och föreslå åtgärder för att garantera en positiv utveckling av datoranvändningen i samhället under demokratisk styrning och kontroll. Häri kan ingå att ta initiativ till utredningsarbete och andra åtgärder som bedöms erforderliga i syfte att bättre kunna följa ADB-utvecklingen inom statsförvaltningen och i samhället i stort. Delegationen bör även kunna få i uppgift att medverka i beredningen av viktigare beslut rörande statlig ADB-verksamhet.

Delegationens bedömningar skulle enligt utskottets mening också kunna vara av värde som en del av riksdagens beslutsunderlag för olika konkreta projekt. Vidare ansåg utskottet att inrättande av en delegation även skulle tillgodose parlamentarisk bevakning av sårbarhets- och säkerhetsfrågor samt ge möjlighet att följa utvecklingen av det allmänna datanätet.

Riksdagen har anslutit sig till utskottets betänkande.

8.1.3 *Vissa utredningar*

Som en uppföljning av de frågor angående samordnad anskaffning av ADB-utrustning som behandlades i princippropositionen har regeringen tillsatt en utredning av frågor rörande samordnad anskaffning av utrustning för ADB i statsförvaltningen (B 1979:09). Vidare har regeringen 1979-06-28 uppdragit åt statskontoret och försvarets rationaliseringsinstitut att utreda frågor rörande anvisningar för ADB samt handlingsprogram för metodstöd. Statskontoret har härutöver 1979-09-27 av regeringen fått i uppdrag att utreda och lämna förslag till åtgärder för att förbättra informationen om användning av ADB i statsförvaltningen m m.

Monopolutredningen (B 1977:08) har i uppdrag att utreda frågan om särställning för vissa myndigheter och företag vid leveranser till staten. I delbetänkandet Konkurrens på lika villkor (SOU 1978:48) anför monopolutredningen bl a att det inte finns anledning att bibehålla den särställning som Statskonsult AB åtnjuter enligt 6 § rationaliseringsför-

ordningen (1957:567). I proposition 1978/79:134 om behandlingen av gällande särställningar för vissa myndigheter vid leveranser till staten m m föreslås bl a att Statskonsult ABs särställning enligt 6 § rationaliseringsförordningen upphävs. I ett andra delbetänkande Datakonkurrens (Ds B 1979:1), avgivet i april 1979, redovisar monopolutredningen sina överväganden angående DAFAs särställning och därmed sammanhängande frågor. Utredningen föreslår att DAFAs särställning upphör i fråga om anpassning av standardprogram som DAFA tillhandahåller, tillhandahållande av färdiga program eller delar av program samt drift av ADB-system (5, 6 och 8 §§ rationaliseringsförordningen).

8.1.4 *Delegationen för vetenskaplig och teknisk informationsförsörjning*

Delegationen för vetenskaplig och teknisk informationsförsörjning har inrättats genom riksdagsbeslut 1978 och 1979. Delegationen skall vara central myndighet för övergripande planering och samordning av informationsförsörjningen till forsknings- och utvecklingsarbete och liknande verksamhet i samhället. Den skall föreslå riktlinjer och åtgärder för att främja en för landet gemensam syn på frågorna om den vetenskapliga och tekniska informationsförsörjningen och verka för att de beslut som regeringen och riksdag fattar inom detta område genomförs. Slutligen skall delegationen ha en övergripande och samordnande uppgift när det gäller att ta initiativ till och främja utbildningen på området samt svara för internationell bevakning och samverkan.

8.2 Näringspolitik och sysselsättningsfrågor

Dataindustriutredningen redovisade i betänkandet Data och näringspolitik 74 (SOU 1974:10) bedömningar rörande allmänna utvecklingstendenser, företagsekonomiska och samhällsekonomiska effekter, sociala effekter, datamarknadens nationella och internationella utveckling inklusive dataindustrin. Vidare behandlades forskning och utveckling, utbildning, dataöverföring, standardisering m m.

I syfte att skapa en konkurrenskraftig svensk dataindustri träffades 1977 avtal mellan staten och SaabScania AB om samarbete på dataområdet i ett nytt gemensamt ägt bolag, Datasaab AB.

Genom regeringsbeslut den 20 juli 1978 har industriverket fått i uppdrag att utreda svensk elektronikindustris nuläge och utvecklingsmöjligheter. Arbetet skall bedrivas i samarbete med styrelsen för teknisk utveckling. I en samma dag inom industridepartementet upprättad promemoria där uppdraget närmare beskrivs heter det bl a att även behovet från försörjningsberedskapssynpunkt bör beaktas. En fördjupad information om hur mindre och med Sverige jämförbara stater bedömer frågor om självförsörjningsgrad och utlandsberoende är i detta sammanhang av stort intresse heter det i promemorian.

Nära anknytning till detta uppdrag har den av regeringen tillsatta kommittén, utredningen om datateknikens och elektronikens effekter på näringslivets utveckling (I 78:04). Enligt direktiven bör kommittén kartlägga i vilken utsträckning näringsliv och samhälle idag utnyttjar datorer eller annan utrustning för avancerad automation, i vilken omfattning detta kan tänkas ske i framtiden och vilken effekt sådan användning kan få på fem, tio och femton års sikt. I uppdraget ingår även att kartlägga vilken produktion av produktionsutrustning som finns inom landet och analys av vilka utvecklingsmöjligheter tillverkare av sådan utrustning kan förväntas ha. Sveriges stora beroende av omvärlden skall särskilt beaktas.

Sysselsättnings- och arbetsmiljöfrågor m m har i viss begränsad omfattning studerats av bl a dataindustriutredningen, datasamordningskommittén samt statistiska centralbyrån i projektet ADB och arbetskraften — slutrapport: Information i prognosfrågor 1977:2. F n studerar en särskilt tillsatt utredning, dataeffektutredningen (A 1978:05), datateknikens effekter på sysselsättning och arbetsmiljö. Utredningen skall enligt direktiven arbeta i nära samband med data- och elektronikkommittén. Sistnämnda kommitté har till uppgift att utforma sitt utredningsmaterial så att det kan tjäna som underlag för dataeffektutredningens närmare analys av sysselsättningseffekterna. Också det material som industriverket tar fram i sitt utredningsarbete av svensk elektronikindustri bör enligt uppdraget kunna tjäna som underlag för närmare analyser av datateknikens effekter på sysselsättningen såväl i verkets egen analys som i dataeffektutredningens analyser av sysselsättningsfrågorna.

Informationsteknologiutredningen (U 1978:12) har till uppgift att studera utvecklingsmöjligheter och problem av ny informationsteknologi såsom text-TV, data-TV och telefaksimil. Utredningen har nyligen avgivit en delrapport Nya Vyer — Datorer och nya massmedier — hot eller löfte? (SOU 1979:69).

Beträffande utnyttjandet av ADB i arbetsförmedlingen m m har riksdagen beslutat (prop 1978/79:131, AU 1978/79:34) bl a om viss utbyggnad av nuvarande försöksverksamhet med sökning och bevakningsmatchning av lediga platser.

8.3 Övriga frågor

8.3.1 *Nationella frågor*

ALLFA-utredningen utreder frågor om ADB inom den allmänna försäkringen. Utredningen har avgivit en lägesrapport ADB inom den allmänna försäkringen på 1980-talet och därefter (Ds S 1979:4).

Riksdagen har vidare nyligen beslutat (prop 1978/79:128, FiU 1978/79:29) att en ny allmän folk- och bostadsräkning skall genomföras under år 1980. Bl a skall bostadsdata inhämtas i samband med att uppgifter under hösten 1980 tas in till 1981 års allmänna fastighetstaxering. Vidare

skall SCB få vissa utredningsuppdrag som bl a syftar till att i framtiden genomföra folk- och bostadsräkningar utan insamling av uppgifter via blankett till allmänheten.

Regeringen har nyligen tillsatt Utredning om den fortsatta fastighetsdataverksamheten (Ju 1979:07). Enligt direktiven skall kommittén bl a utreda skilda system för fastighetsregistrering och inskrivningsväsendet men även undersöka andra lösningar och däribland även sådana som bygger på driftsystem 1 vilket är i drift i en del av landet. I samband härmed bör kommittén pröva frågan om en regionalisering eller annan geografisk spridning av datordriften. Den bör med beaktande bl a av sårbarhets- och integritetssynpunkter undersöka och bedöma olika alternativ i detta hänseende. Kommittén bör vidare enligt direktiven behandla bl a frågor om koordinatregistreringen och databearbetningar som sker med hjälp av de registrerade koordinaterna.

ADB-beredningsgruppen (C 1973:06) behandlar frågor om utveckling och utnyttjande av ADB i samhällsplaneringen. Gruppen har avgivit en lägesrapport ADB i samhällsplaneringen (Ds Kn 1976:1-2) och betänkandet ADB i den regionala samhällsplaneringen (Ds Kn 1976:7).

Tilläggsdirektiv har nyligen givits för ADB-beredningsgruppen (dir 1979:103). Enligt direktiven skall gruppen bl a utarbeta ett konkret förslag till en samlad lösning för den regionala och lokala samhällsplaneringens informationsförsörjning. Gruppen skall lägga särskild tonvikt vid utnyttjande av befintlig information från register som har skapats för olika samhälleliga ändamål. Enligt direktiven torde de register som byggs upp för angivna ändamål komma att ge en samlad bild av olika förhållanden i länen. Det är därför nödvändigt att beredningsgruppen särskilt beaktar integritetsskravet samt undersöker hur registren skall kunna skyddas, undanföras eller förstöras vid krig eller krigsfara. Beredningsgruppen skall även uppmärksamma frågan om länsstyrelsernas användning av ADB i den egna aministrationen. Vidare skall beredningsgruppen utreda och lämna förslag till hur datorutnyttjandet för samhällsplaneringen skall samordnas med motsvarande ansvar för folkbokförings- och skattesystemet.

8.3.2 *Internationellt samarbete*

Såväl nationellt och internationellt aktualiseras i samband med den ökade överföringen av data mellan olika länder frågor angående bl a nationell suveränitet, integritetsskydd, sårbarhet, säkerhet, sekretess samt nationalekonomiska och sociala effekter. Internationellt arbete vari Sverige deltar bedrivs rörande bl a problem och effekter av dataflöde över gränserna inom Nordiska rådet, OECD och Europarådet.

Inom OECDs Committee for Scientific and Technological Policy (CSTP) följs utvecklingen på datateknikens och elektronikens område. En av arbetsgrupperna under CSTP, Working Party on Information, Computer and Communication Policy (ICCP) behandlar bl a frågor om dataflöde över gränserna, datanätspolitik, integritetsskydd, sårbarhet, information för industrins behov, ekonomiska och sociala effekter av

informationsteknologin, nationell datapolitik i medlemsländerna samt överföring av information till utvecklingsländer.

Inom ICCP planeras en High Level Conference on Information Computer and Communication Policy for the 1980s som skall äga rum i mars 1980. Vid konferensen kommer frågor inom ICCP-området bl a sårbarhetsfrågor att behandlas men på en högre politisk nivå. Huvudsyftet med konferensen är att medlemsländerna skall utbyta idéer och erfarenheter på området och närmare ange vilka frågor som bedöms mest väsentliga för framtida OECD-arbete och vilken roll OECD därvid skall spela.

Inom ICCP ges högsta prioritet till arbetet med att utarbeta riktlinjer för dataflöde över gränserna och skyddet för persondata och personlig integritet. Detta arbete skall vara avslutat under 1979. Härefter skall de juridiska och ekonomiska problem som kan uppkomma när andra data än persondata överförs mellan länder undersökas.

Jämsides med arbetet i OECD pågår arbete inom Europarådets dataskyddskommittee med att utarbeta en konvention om skydd för persondata och personlig integritet. Även detta arbete skall vara avslutat under 1979.

Avslutningsvis kan nämnas att den svenska datalagstiftningskommittén har till uppgift att lägga fram förslag till de lagbestämmelser som föranleds av internationella överenskommelser eller som annars påkallas av hänsyn till den internationella datatrafiken. Detta uppdrag är inte begränsat till personuppgifter.

8.3.3 *Internationella datanät*

De nordiska televerken installerar f n ett gemensamt nordiskt allmänt datanät (NPDN). Detta utnyttjar speciella ledningar i det allmänna telenätet och på speciella elektroniskt styrda växlar. Systemet arbetar med s k genomkopplade förbindelser mellan sändare och mottagare (circuit switching). Bland de första tjänster som kommer att anslutas är penninguttagsautomater och betalningsautomater för drivmedel. Televerken planerar vidare en speciell datanätstjänst för utnyttjare av datorbaserade informations- och dokumentationstjänster. Denna bygger på en annan kopplingsteknik, paketförmedling (packet switching).

Inom den europeiska gemenskapen pågår likaledes installationer av ett speciellt enhetligt datanät, Euronet, primärt avsett för informations- och dokumentaionsändamål. Förhandlingar pågår om anslutning mellan Euronet och det svenska nätet i syfte att ge användare och leverantörer tillgång till en större internationell informationsmarknad.

9 Behandling av sårbarhetsfrågor i vissa främmande länder

Av redovisningen under 8.3.2 ovan framgår att visst internationellt samarbete pågår beträffande sårbarhetsfrågor. Detta är tecken på ett ökande intresse för dessa frågor även i andra länder än Sverige. Emellertid har inte — såvitt bekant — några övergripande offentliga utredningar om det datoriserade samhällets sårbarhet gjorts utomlands. I Finland har dock en kommittee tillsatts med uppdrag bl a

- att finna vägar att minska sårbarhet som beror på ADB-användning
- att avgöra vilka system som är vitala för samhället
- att för dessa system se till att säkerhetsåtgärder vidtas och katastrofplaner upprättas.

Många av de delfrågor som SÅRK arbetar med har varit föremål för ingående diskussioner utomlands t ex de risker som följer av olika slags brottslighet riktad mot ADB-verksamhet. Det kan i detta sammanhang nämnas att i USA lades i januari 1979 fram ett förslag till kongressen om att införa särskilda straffbestämmelser — med väl tilltagna straffsatser — för olika slags databrott. I förslaget sägs bl a att databrott är ett växande problem och att sådant brott ofta medför större förluster än andra typer av förskingrings- och bedrägeribrott.

I en kanadensisk rapport från januari 1979, Security in the EDP Environment, diskuteras sårbarhetsfrågor. Bl a framhålls vikten av att skydda känslig information och vikten av att system inom funktionellt känsliga samhällssektorer fungerar. I rapporten anges bl a koncentration, komplexitet och beroendet av nyckelpersoner för ADB-driften som viktiga sårbarhetsfaktorer. Vidare diskuteras olika säkerhetsåtgärder som bör vidtas. I rapporten framhålls slutligen vikten av kontinuerlig katastrofplanering.

Det kan även nämnas att kanadensiska politiker och tjänstemän uttalat stark oro över det ökande beroendet av ADB-bearbetningar utomlands, främst då i USA. Man har till och med ställt frågan om detta beroende kan vara ett hot mot landets suveränitet. Några av de negativa effekter man pekar på är att stora mängder information — både personuppgifter och andra uppgifter — kommer utom räckhåll för kanadensisk lag och att viktiga beslut för bl a landets näringsliv kan komma att fattas utomlands. Vidare diskuteras effekter som förlusten av arbetstillfällen, påverkan i negativ riktning av bytesbalansen, integritetsrisker m m.

Redan 1975 utfärdade den australiensiska regeringen riktlinjer beträf-

fande nationell säkerhet och säkerhetskrav vid användningav ADB-tjänster utomlands. Man konstaterade att problem kunde uppstå om en tvist eller intressekonflikt skulle uppstå mellan statliga användare och anlitad servicebyrå, något som möjligen kunde leda till att användarens data inte lämnades ut eller att användaren vägrades olika tjänster.

I Frankrike skärpte man i december 1976 den instruktion som rör skyddet av försvarshemligheter. Skälet till detta var att man såg nya risker i den ökande användningen av datorer. Bland riskerna nämndes bl a ökade möjligheter för obehöriga att ta del av stora informationsmängder, och ökade möjligheter att manipulera och förstöra information. Man pekade även på att ADB-bearbetningar av i och för sig öppna uppgifter många gånger kan ge information som bör skyddas.

I Norge utfärdades hösten 1978 ett första utkast till direktiv för datasäkerhet i statsförvaltning. Direktiven skall komplettera säkerhetsföreskrifter av mera allmän karaktär från 1972 och gäller beträffande s k graderade datasystem, vilket innebär att systemen innehåller känslig information eller på annat sätt har säkerhetsmässig betydelse. I utkastet diskuteras en del av de sårbarhetsfaktorer som SÅRK tagit upp i sin lägesrapport. Som exempel kan nämnas kriminella handlingar av typ spioneri och sabotage; beredskapssituationer och krig varvid även EMP-effekter nämns. Vid diskussion av spioneribrotten sägs att i underrättelseverksamhet insamlas upplysningar numera inte bara om aktuella försvars- och beredskapsplaner utan även om politiska förhållanden, teknik och vetenskap, näringsliv, industri, ekonomi, kommunikationer, sociala förhållanden, enskilda personer osv. Detta underlättas genom att stora mängder sådan information finns lagrad på datamedium. Andra faktorer som diskuteras är beroendet av pålitlig personal, risker för obehörig avtappning av information och obehörig avlyssning, risk för oavsiktliga fel och misstag, skador på grund av brand, översvämning, avbrott i kraftförsörjningen etc.

I direktiven diskuteras sedan olika åtgärder som måste vidtas för att en rimlig säkerhetsnivå skall kunna uppnås. Hit hör dokumentationens betydelse, behovet av back-up rutiner och katastrofberedskap samt användning av kryptering och behörighetssystem. Även frågor som rör datatekniska lösningar tas upp och bl a pekar man i rapporten på nackdelar från säkerhets- och sårbarhetssynpunkt med s k blandad drift. Även utformningen av program med utgångspunkt från säkerhetsaspekten ägnas uppmärksamhet. Vidare diskuteras behovet av skärmning som skydd mot elektromagnetisk utstrålning. Sådan strålning ger möjlighet till avlyssning. Skärmning för detta ändamål kan, om den byggs ut, även ge skydd mot EMP-effekter vid atombombsexplosioner heter det i direktiven.

Hittills har emellertid huvudintresset i olika länder varit riktat mot integritetsfrågor och i ett antal stater har lagstiftning skett eller pågår lagstiftningsarbete inom detta område. De lagar som kommer till i syfte att skydda personlig integritet bidrar i regel även till att minska sårbarheten i vissa avseenden. I de flesta lagar finns t ex bestämmelser, som begränsar rätten att registrera känslig information och om ADB-säker-

het. I vissa lagar finns bestämmelser som tar sikte på utlandsbearbetningar. Lagstiftningen i en del länder är inte begränsad till olika ADB-register utan omfattar även känsliga manuella register. Vidare har en del länder låtit lagstiftningen inte enbart omfatta fysiska personer utan även juridiska personer.

För närvarande finns datalagar, förutom i Sverige, i bl a Kanada, Förenta Staterna, Danmark, Österrike, Frankrike, Luxemburg, Norge, Förbundsrepubliken Tyskland och Ungern. Lagstiftningsarbete pågår i bl a Belgien, Spanien, Nederländerna och England. I Kanada och USA är det endast den offentliga sektorn som är reglerad. I Danmark finns två lagar, en för den offentliga och en för den privata. Lagarna i Kanada, Förenta Staterna, Norge och Frankrike rör även vissa manuella register. Till de länder som låtit såväl fysiska som juridiska personer omfattas av lagstiftningen eller förslag till sådan hör Österrike, Belgien, Danmark (privatsektorn), Luxemburg och Norge. Skydd ges således även beträffande juridiska personer även om lagarna primärt tar sikte på att skydda den enskildes privatliv och integritet.

Som nämnts bidrar integritetsskyddslagstiftning i flera avseenden även till gynnsamma effekter vad gäller sårbarhet. I utländsk datalagstiftning kan man även finna vissa bestämmelser, som åtminstone enligt svenskt synsätt rör sårbarhetsaspekter. Som exempel kan nämnas att den franska datalagen ger tillsynsorganet rätt att vid extraordinära förhållanden ge föreskrifter bl a om förstöring av datamedier. Med extraordinära förhållanden avses bl a att det föreligger risk för en statskupp.

Det kan även nämnas att vid tillkomsten av den norska lagen diskuterades en sårbarhetsfråga av speciell art. I lagens 4 § finns en bestämmelse om att datatillsynet — den norska motsvarigheten till datainspektionen — skall föra en systematisk förteckning över tillståndspliktiga personregister. Förteckningen, som skall finnas tillgänglig för envar skall innehålla uppgift om registeransvarig, vilken typ av upplysningar registret innehåller och vad det skall användas till. Vid remissbehandling av de betänkanden som låg till grund för propositionen pekade några instanser på de risker från beredskapssynpunkt och med hänsyn till rikets säkerhet som en sådan förteckning kunde medföra. En remissinstans anförde bl a att en sådan förteckning kan vara till ovärderlig nytta för den som vill skapa kaos eller överta kontrollen över väsentliga delar av samhällsapparaten.

Dessa synpunkter beaktades och i 4 § sista stycket i lagen har regeringen givits rätt att göra de undantag från huvudregeln som är nödvändiga från beredskapssynpunkt eller med hänsyn till rikets säkerhet.

IV SÅRKs överväganden

10 Allmänna överväganden

10.1 Inledning

SÅRK har utgått från att det tekniskt utvecklade samhället inte kan undvara ADB-tekniken och att användning av ADB har många och stora fördelar för samhället. Samtidigt har SÅRK pekat på en mängd sårbarhetsfaktorer och risker som hör samman med ADB-användning. Den redovisning som gjorts i det föregående kan — bl a på grund av den kumulativa effekt som en riskkatalog ger — bidra till ett alltför pessimistiskt synsätt på hur sårbart samhället har blivit på grund av datoriseringen. Många av de faror och risker som målats upp är av den art att det är ganska osannolikt att de skall bli verklighet.

Kartläggningen leder emellertid 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 såväl för krigs- och beredskapssituationer som för förhållanden under fredstid. Olika händelser och angrepp kan ge omfattande störningar och skador även vid djupaste fred.

Dessa allmänna slutsatser har förts fram i SÅRKs lägesrapport och har vid remissbehandlingen godtagits av en överväldigande majoritet av remissinstanserna.

10.2 Det moderna samhällets allmänna sårbarhet

I diskussionen kring samhällets sårbarhet på grund av den tilltagande datoriseringen framförs ofta konstaterandet att ADB är endast en av orsakerna till en ökad allmän sårbarhet hos samhället. Liknande synpunkter har framförts i remissyttrandena över SÅRKs lägesrapport. SÅRK vill därför kortfattat belysa denna fråga i syfte att anlägga ett riktigt perspektiv beträffande samhällets sårbarhet på grund av datoriseringen.

Ett modernt högindustriellt välfärdssamhälle är allmänt sett väsentligt mer sårbart än andra. En mängd olika sårbarhetsfaktorer förekommer inom det egna landet. Andra härrör från förhållanden utanför landets gränser. Några exempel kan åskådliggöra detta.

Energiberoendet är mycket stort. En omfattande oljeimport till rimligt pris är i nuläget en förutsättning för industrins kraftförsörjning, för nuvarande kommunikationsmönster och för bostadsuppvärmning. Det moderna samhället är också i hög grad beroende av en fungerande eldistribution liksom telenät m m.

Import av råvaror som vissa metaller, rågummi, olja och gödningsämnen är också en förutsättning för nuvarande produktion inom t ex metall- och plastindustrierna, annan verkstadsindustri samt inom jordbruket.

Även när det gäller halvfabrikat och reservdelar är importberoendet stort på många områden. Således är svensk bilproduktion starkt beroende av import av vitala delar som växellådor eller t o m smärre plastdetaljer. Inom jordbruket föreligger ett starkt beroende av import av reservdelar till traktorer och andra redskap.

Denna situation är en följd av vårt handelsutbyte. Vår export har varit och är alltjämt en viss garanti för en fortlöpande import. Tidigare framstående svenska exportprodukter tillverkas emellertid numera även i andra länder till låga priser.

Krigshändelser — antingen de direkt berör vårt land eller inträffar mellan länder från vilka vi är beroende av en ostörd import — kan leda till dramatiska sårbarhetseffekter. Sådana effekter kan dock uppkomma redan genom handelspolitiska åtgärder som begränsningar i oljeimporten genom minskad produktion i eller försäljning från de oljeproducerande länderna. Erfarenhetsmässigt vet man att effekter av detta slag kan inträffa även genom förändrad prispolitik.

Det tekniskt präglade samhället är beroende av specialister. Sårbarhetseffekter, om än ofta begränsade, kan uppstå genom störningar på arbetsmarknaden inom det egna landet eller i andra länder.

Välfärdssamhällets speciella sårbarhet hänför sig också till medborgarnas höggradiga beroende av samhället samt till den långtgående integration som förekommer inom och mellan olika samhällsfunktioner. Sociala reformer kräver en omfattande administration och stora penningflöden. Störningar häri kan vålla betydande avbräck.

Det tekniskt komplicerade samhällets sårbarhet kräver skyddsåtgärder mot t ex terroristhot. Inom energiproduktionen krävs särskilda skyddsåtgärder i synnerhet vid kärnkraftsanläggningar. På motsvarande sätt behöver inom administrationen skydd skapas för centrala datoranläggningar. Utomlands finns exempel på att sådana skyddsåtgärder ansetts böra drivas så långt att de knappast kan anses förenliga med de demokratiska värderingar vi betraktar som väsentliga. Samtidigt som demokratin som sådan utgör ett skydd mot explosioner av social karaktär, som kan ge upphov till att olika grupper försöker störa viktiga samhällsfunktioner, har en demokrati svårigheter att i alla lägen tillåta de skyddsåtgärder som den uppkomna sårbarheten i och för sig skulle motivera.

Samhället strävar fortlöpande efter att begränsa sårbarhetsfaktorerna allteftersom sådana uppmärksammas. För att minska sårbarheten förekommer bl a en omfattande lagring av vissa produkter. Beredskaps-

lagring förekommer således till betydande kostnader av råvaror som olja eller vissa livsmedel, av vissa färdiga produkter, exempelvis läkemedel och textilprodukter. Samtidigt bedrivs arbete inom landet på att utveckla ersättningsprodukter som gengasaggregat m m. Beredskap upprätthålls i form av tekniskt kunnande i syfte att kunna tillverka sådana produkter som inte behövs i fredstid och tillverkningsvertyg hålls tillgängliga för att produktion snabbt skall kunna komma igång.

De angivna exemplen visar klart att ADB-användningen endast är en bland flera orsaker till det moderna samhällets sårbarhet. Detta förhållande får emellertid inte godtas som ursäkt för att underlåta att begränsa sårbarhet betingad av ADB-användning så länge en sådan begränsning kan uppnås med rimliga medel. Tvärtom är det enligt SÅRKs mening ytterst angeläget att motåtgärder snarast vidtas för att minska den tilltagande sårbarhet som föranledes av samhällets datorisering. Därmed uppnås även en minskning av samhällets totala sårbarhet.

10.3 Sårbarhet beroende på ADB-användning

När det gäller ADB föreligger — såsom ovan beskrivits — ett betydande importberoende och en därav följande sårbarhet. Importberoendet omfattar i första hand datorer och reservdelar till dem. Det omfattar emellertid även betydande kringutrustning och komponenter till sådan. Det förekommer t o m ett importberoende beträffande sådana till synes triviala detaljer som färgband till utskriftsapparater.

Importberoendet omfattar också tekniskt kunnande (know how) för installationer av datorer, programvara, behörighetssystem, felsökning och reparation. I vissa fall synes felanalyser f n endast kunna ske utomlands hos tillverkarna av datorer.

Till detta kommer ett inte obetydligt importberoende av datatjänster i form av bearbetningar av information utomlands. En stor del av verksamheter med internationell prägel kräver samverkan i fråga om datatjänster. Exempelvis är den internationella flygtrafiken på ett avgörande sätt beroende av det s k SITA-systemet. Inom bankverksamhet föreligger likartat beroende av det s k SWIFT-systemet. Beroende av utländska datatjänster föreligger även beträffande många svenska företags lagring och bearbetning av data för administation och produktionsstyrning.

Vid sidan av detta utlandsberoende står ett flertal sårbarhetsfaktorer att finna inom landet.

Den hittills genomförda datoriseringen har gett upphov till risker i varierande frekvens av en mängd olika slag. Till de mindre riskerna för fel och störningar räknas sådana som orsakas av skador till följd av storm, översvämning, brand m m. Sannolikheten för störningar i dessa avseenden är — till skillnad från olyckshändelser i driften av datasystem eller avsiktligt åstadkomna fel och störningar — ganska låg. Trots detta är de värda att beakta vid inrättandet av datacentraler.

Beredskapen mot kriminella handlingar, missbruk för politiska syften och krigshandlingar är många gånger obefintlig eller i vart fall otillräck-

lig. Som exempel kan nämnas den ekonomiska brottslighet där datorer utnyttjats som hjälpmedel. I de hittills kända fallen — nästan undantagslöst upptäckta av en slump — har det vanligen gällt mycket stora värden.

Datoriseringen har medfört funktionellt känsliga system både inom administration och produktion. Vidare har ADB-driften koncentrerats både funktionellt och geografiskt på sätt som knappast vittnar om att sårbarhetsfaktorer beaktats. Genom anhopningen av datorkraft till storstäderna har den geografiska koncentrationen blivit alltför stor. Den funktionella koncentrationen är resultatet av anhopningar av information till centrala system hos speciella myndigheter eller till stora servicebyråer med många kunder. Koncentrationen i olika former ökar datacentralernas betydelse som mål för störningar.

De risker koncentrationen vållat har förstärkts genom en långt driven integration mellan framförallt de centrala systemen. Det inbördes beroendet uppstår redan när ett system måste få tillgång till grunddata från ett annat. Beroendet kompliceras emellertid ytterligare genom mera omfattande informationsutbyte och genom tekniska hopkopplingar som t ex vid dator till dator-förbindelser. Integrationen förstärker effekten av ett strategiskt angrepp mot datacentraler.

Enligt SÅRKs uppfattning föreligger sårbarhet främst beträffande de stora centrala systemen och datoranläggningarna, till vilka SÅRK även räknar de stora servicebyråerna. Detta gäller trots att de från ekonomisk utgångspunkt kan förses med ett mer omfattande skydd än de små. De är i princip utsatta för flertalet av de risker som SÅRK funnit anledning att belysa i det föregående. Deras storlek innebär bl a att en olyckshändelse lätt kan få karaktären av katastrof. I de centrala systemen ingår vanligtvis innehållsmässigt känsliga register. De är ofta dessutom funktionellt känsliga. Samtidigt som den geografiska och funktionella koncentrationen i ekonomiska avseenden medger bl a ett bättre fysiskt skydd än regionalisering och decentralisering får man inte glömma att det är koncentrationen som nödvändiggör stor del av skyddsåtgärderna. Det är en uppenbar risk, i vart fall på sikt, att dessa skyddsåtgärder kommer att vara svåra att förena med ett demokratiskt synsätt bl a genom att de hindrar insyn och ställer krav på alltför långtgående kontrollåtgärder beträffande personal. Den funktionella och geografiska koncentrationen medför att de centrala systemen utgör lockande mål för dem som genom kriminella handlingar önskar störa vitala samhällsfunktioner eller bara vill vidta åtgärder i vinningssyfte. I krigshänseende torde det vara en realistisk bedömning att presumtiva angripare kan betrakta vissa centrala system som mål för angrepp. Integrationen och det inbördes beroendet förstärker riskerna i betydande omfattning. Nödvändigheten av en mängd olika skyddsåtgärder alltifrån starkt fysiskt skydd till kryptering gör databehandling till en sluten miljö med de risker detta kan medföra genom att normal insyn försvåras.

Ansamlingen av stora datamängder och möjligheten att centralt bearbeta dem underlättar manipulation av information samt politiskt missbruk. De stora datamängderna har dessutom föranlett oro inom näringslivet som uttalat önskemål om ett skydd för företagens integritet eller

med andra ord ett förbättrat skydd för juridiska personer mot bl a industrispionage[1]. Centraliserade system underlättar kanske rekrytering av kompetent personal men alltjämt är beroendet av nyckelpersoner ofta för stort. Bidragande härtill är komplexiteten i systemen, bristfällig dokumentation och utbildning m m.

10.4 Orsaker till rådande förhållanden

Datoriseringen av det svenska samhället har skett genom en snabb utveckling under 1960- och 1970-talen. Övergång till ADB-system inom den statliga sektorn har ofta skett efter beslut inom enskild myndighet, även om regering och riksdag haft avgörandet i fråga om anskaffning av ADB-anläggningar och datorisering av sådana rutiner där själva övergången till ADB krävt särskilda anslag eller ändringar i gällande lagstiftning. På den privata sidan har datoriseringen naturligt nog skett efter beslut hos det enskilda företaget.

Efter datalagens ikraftträdande har datainspektionen haft en prövningsrätt i tillståndsärenden och en tillsynsskyldighet i fråga om ADB-verksamhet. Prövnings- och tillsynsverksamheten har emellertid varit begränsad till integritetsaspekter och gällt endast personregister.

Från statsmakternas sida har inte skett någon styrning av den utveckling som lett fram till dagens genomdatoriserade samhälle. Utvecklingen har rullat vidare utan att någon övergripande bedömning gjorts av de risker som den sammantagna datoriseringen av olika samhällsområden leder till. Någon helhetsbedömning av situationen har inte funnits ens inom den statliga sektorn och än mindre för hela samhället. Ej heller har några riktlinjer meddelats. Detta torde främst ha sin förklaring i en bristande medvetenhet om och förutseende beträffande sårbarhetsproblem förknippade med ADB-utvecklingen. Ibland när sådan medvetenhet förelegat har tids- eller kostnadsskäl bidragit till att de ej tillräckligt beaktats.

På vissa punkter inom den statliga verksamheten har funnits normer som varit tillämpliga ifråga om utvecklingen av ADB-verksamheten. Enligt kungörelsen (1966:273) om säkerhetskydd vid statsmyndigheter skall statsmyndighet som har befattning med uppgift eller förhållande som angår rikets försvar eller landets säkerhet i övrigt vidtaga åtgärder för säkerhetsskydd inom sitt verksamhetsområde. Gällande föreskrifter för statliga myndigheters planläggning av informationsbehandling i krig (återgivna under 4.3.3 ovan) reglerar flera av de frågor om krigsplanering som behandlas av SÅRK. Även på de områden där föreskrifter finns att tillgå förefaller sårbarhetsproblemen vara föga uppmärksammade. När de väl uppmärksammats visar erfarenheterna att det varit mycket svårt för projektansvariga att få tillgång till framtagna normer, att dessa varit otillräckliga och att det saknats någon form av samlande rådgivning.

Den bristande medvetenheten om sårbarhetsproblem är inte unik för Sverige. I den internationella debatten är det först på senare år som dessa problem fått någon egentlig uppmärksamhet.

[1] Se Industriförbundets skrivelse, refererad under avsnitt 5.1.2 ovan

ADB-tekniken anses av många alltjämt befinna sig i ett inledningsskede. Detta påstående torde i vart fall stämma beträffande omfattningen av användningen av ADB. Redan i dagsläget satsas emellertid avsevärda resurser på ADB-användning. Enligt riksrevisionsverkets rapport Tio myndigheters ADB-verksamhet — styrning, kostnader m m, uppgick de totala direkta kostnaderna för ADB-verksamheten bara inom statsförvaltningen under budgetåret 1977/78 till 1 197 milj kr. Motsvarande belopp beräknades under budgetåret 1978/79 stiga till 1 382 milj kr.

Allmänt torde gälla att utnyttjande av komplicerad och avancerad teknik efterhand skapar ett kraftigt beroende av denna teknik. Mot bakgrund av de gjorda investeringarna blir av ekonomiska avskrivningsmässiga skäl en återgång till tidigare utnyttjade hjälpmedel svår. Vidare föreligger ofta från ADB-användarens sida en bristande benägenhet att erkänna misstag i fråga om införande av ADB-system. Ett visst prestigetänkande gör det svårt att överge ett system som egentligen inte borde ha införts. I en del fall genomförs inte utvärdering av ADB-system på sådant sätt att användaren får klart för sig om systemet bör läggas ner eller inte. Detta drag av oåterkallelig utveckling hos den nya tekniken förstärks av utnyttjandet av dess nya möjligheter. Det torde knappast finnas någon återvändo till manuella system antingen det gäller processstyrning eller stora administrativa system. Om inte en återgång noga planerats skulle man säkerligen efter en kaotisk situation få börja om från början. Effekten förstärks också om t ex utnyttjandet av tekniken i det enskilda fallet blir beroende av andra användares tekniska lösningar som är fallet vid upprättandet av fasta samkörningsrutiner mellan olika ADB-system.

De problem SÅRK kartlagt och bedömt nödvändiga att åtgärda har flera orsaker. Den grundläggande orsaken ligger i att man inte förmått förutse sårbarhetseffekterna och därför inte kunnat beakta dem. En annan orsak är storskaligheten. Under ADB-teknikens första årtionden producerades endast generella datorer med en ständigt ökande kapacitet. Dessa datorer inbjöd till centrala integrerade system. Storskaligheten betraktades som rationell och ekonomisk. Trots att det, enligt SÅRKs uppfattning, endast finns ytterst få om ens några sådana system som kunnat införas utan tekniska problem har denna utveckling fortsatt. Exempelvis har fastighetsdatasystemet mer än tio år efter beslutet om genomförande en produktion som bara omfattar en liten del av landets fastighetsbestånd. Förklaringen till att denna utveckling mot storskalighet alltjämt fortsätter är sannolikt bl a de mycket stora investeringar som gjorts i datorer och systemlösningar samt inrättandet av administrativa organisationer som synes svåra att förändra i takt med och vunna erfarenheter.

Trots att den fortsatta ADB-tekniska utvecklingen numera medger helt andra lösningar kommer det att ta mycket lång tid att förändra strukturen på dagens ADB-användning. Minidatorer och mikroprocessorer kan inte ersätta alla generella datorer. Samtliga större system beroende av andra går f ö sannolikt inte att avveckla. Om man skulle

önska en snabb avveckling av många nu centrala system är gjorda investeringar och integrering av systemen ett avgörande hinder mot en sådan avveckling. De kan knappast avvecklas på kortare tid än det tagit att utveckla dem. Snarare kommer det att ta längre tid. Förändringar i strukturen hos de statliga systemen blir i viss mån vägledande för stora delar av näringslivet som sannolikt kan väntas anpassa sina system därefter för att kunna möta kraven på insamling av information till den offentliga sektorn och kunna utnyttja återflödet från denna.

Ett annat skäl till nuvarande situation är den allmänna knappheten på personella resurser. Vanligtvis har inte de personella resurserna räckt till för att under de ofta av stor optimism präglade tidsberäkningarna åstadkomma en nödvändig och allsidig systemutveckling. Under dessa betingelser är det helt naturligt att systemutvecklingsarbetet, som är krävande och fyllt av problem inte förenats med alla de bedömningar SÅRK nu finner påkallade. Det har dessutom saknats tillsyn över systemutvecklingsarbetet såvitt gäller sårbarhetsaspekter. En sådan tillsyn borde ha ålegat något organ utanför ADB-användarens egen organisation.

10.5 Åtgärder för att motverka sårbarheten

10.5.1 *Principiella överväganden*

Remissyttrandena över SÅRKs lägesrapport visar dels att de kartlagda problemen inte är helt nya dels att en överväldigande majoritet av remissinstanserna, som genom lägesrapporten uppmärksammats på problemen, påkallar att åtgärder vidtas för att lösa problemen. Dessa intryck förstärks av förfrågningar under hand till SÅRK om när sådana åtgärder kan väntas. Man efterlyser helt enkelt ett samhällsansvar på detta område. Samtidigt är det anmärkningsvärt att sårbarhetsfrågorna i så ringa omfattning fått sätta sin prägel på beslut om systemutveckling.

Behovet av insatser för att motverka risker för skadliga effekter är inte unikt för ADB-tekniken. Krav på säkerhet och trygghet ställs både av de enskilda medborgarna och samhället i många olika sammanhang. Som exempel kan nämnas byggnadsverksamhet, sjöfart, flygtrafik och vägtrafik. Andra exempel på områden där medborgaren och samhället ställer stora krav på trygghet är kärnkraft, hälso- och sjukvård, miljövård och eldistribution. På samma sätt som beträffande beredskapsåtgärder på andra områden är det nödvändigt att åtgärder vidtas beträffande användningen av ADB.

ADB-tekniken har medverkat till utvecklingen av en helt ny industri, informationsindustrin. Denna består inte bara av datortillverkare utan även företag som tillhandahåller mjukvara, datatjänster osv. Många betraktar dagens samhälle som det postindustriella informationssamhället. I informationsindustrin tillverkas och förädlas information, som fått ett egenvärde. De skador som kan vållas av en enskild operatör i en större datacentral uppgår till avsevärda belopp.

SÅRK har tidigare framhållit att ADB-användningen starkt präglas av att en återgång till tidigare arbetsmetoder är praktiskt taget omöjlig. Detta leder till att det är särskilt angeläget att så långt möjligt undvika de problem beträffande datoriseringens inverkan på samhällets sårbarhet som SÅRK funnit. Enligt SÅRKs uppfattning kan sårbarheten begränsas i redan existerande system. Nya system bör genom en sårbarhetsbedömning kunna byggas upp annorlunda än hittills skett.

Detta mål kan delvis uppnås genom information och rådgivning. Redan den allmänna diskussion som SÅRKs lägesrapport framkallat har fäst ADB-användarnas uppmärksamhet på sårbarhetsproblemen och även ökat användarnas intresse för att lösa dessa problem. Enligt SÅRKs mening är emellertid information och rådgivning inte tillräckligt verksamma medel beträffande sådan datoranvändning som är särskilt betydelsefull från sårbarhetssynpunkt. Såsom närmare utvecklas i följande avsnitt är det nödvändigt med en allmän sårbarhetsprövning beträffande vissa sektorer av datoranvändningen. En sådan prövning bör omfatta

- registerinnehåll
- systemstruktur
- ADB-säkerhet dvs kapitalskydd, dataskydd, funktionsskydd och kvalitetsskydd
- personalberoende
- maskinella och manuella reservrutiner
- behov och förekomst av plan för olika krisnivåer
- dokumentation
- beroendet av andra databehandlingssystem utanför den egna verksamhetens organisation
- geografisk lokalisering
- lämpligheten av utlandsbearbetningar

Först om en samlad bedömning av samtliga dessa punkter leder till slutsatsen att systemet har en tillfredsställande nivå ifråga om säkerhet bör det få tas i drift.

En del av ovanstående punkter kan göras till föremål för teoretiska sannolikhetsbedömningar varigenom man kan utvärdera och jämföra olika alternativ i kvantitativa termer. De flesta punkterna kan emellertid endast underkastas en kvalitativ bedömning.

En sammanvägning av de olika faktorerna till en total sårbarhetsbedömning kan likaledes enbart göras i kvalitativa termer.

Liksom SÅRK anser att det står klart att sårbarheten på några håll är oacceptabelt hög, står det också klart att sårbarhetsreducerande åtgärder inte får orsaka oacceptabla merkostnader vare sig för de granskade systemen eller för granskningsfunktionerna.

Beträffande servicebyråer bör prövningen begränsas till de punkter för vilka ansvaret helt eller delvis naturligt ligger på servicebyrån. Däribland ingår främst ADB-säkerhet, personalberoende, dokumentation, reservrutiner, katastrofplaner och utlandsbearbetningar.

Den nu skisserade sårbarhetsprövningen förutsätter någon form av ansöknings- och tillståndsförfarande. I det följande kommer SÅRK att

bedöma vilka sektorer av ADB-användning som bör vara underkastade sådant förfarande. Vid bedömningen görs en avvägning mellan å ena sidan de krav sårbarhetssituationen ställer och å andra sidan vad som är realistiskt från ekonomisk och praktisk synpunkt. Bedömningen utgår från att tillståndsförfarandet inte skall omfatta större del av samhällets ADB-användning än vad som är oundgängligen nödvändigt. Dessa överväganden leder för det första fram till att stora delar av ADB-användningen inom både den offentliga och privata sektorn helt kan lämnas utanför en sårbarhetsprövning. För det andra bör man enligt SÅRKs mening — i vart fall för närvarande — stanna vid ett anmälningsförfarande beträffande större delen av den ADB-användning inom den privata sektorn som är av betydelse från sårbarhetssynpunkt. Anmälningsförfarandet fyller ett dubbelt syfte: anmälningarna bildar underlag dels för rådgivning i det särskilda fallet dels för en framtida bedömning huruvida mer ingripande åtgärder — exempelvis tillståndsförfarande — kan anses påkallade.

Den allmänna sårbarhetsprövning som SÅRK sålunda föreslår bör kombineras med tillsyns-, rådgivnings- och informationsverksamhet. Detta utvecklas närmare under avsnitt 16.

Beträffande utlandsberoende, personalberoende och vissa andra sårbarhetsfaktorer föreslås i avsnitt 18 speciella åtgärder.

10.5.2 *Olika åtgärder*

SÅRK har i tidigare avsnitt konstaterat att sårbarheten är oacceptabelt hög i dagens genomdatoriserade samhälle och att den fortgående utvecklingen på väsentliga områden leder till en allt högre sårbarhet i framtiden om inte motåtgärder vidtas. Vad som erfordras är, enligt SÅRKs mening, ett samhällsansvar på detta område.

Den hittillsvarande regleringen av datoranvändning har i huvudsak gällt integritetsfrågor och system med personinformation. Redan denna reglering har inneburit att ett stort antal olika verksamhetsområden i samhället har berörts i större eller mindre omfattning. Sårbarhetsaspekten torde ha ännu fler beröringspunkter med olika samhällsföreteelser. Som visats finns en mängd information av annat slag än personinformation av betydelse vid sårbarhetsbedömningar. Det kan t ex gälla uppgifter om företag, fastigheter, vägar, broar och det kan gälla annan landskapsinformation m m. Vidare används datorer alltmer som hjälpmedel i processindustri, grafisk industri, vid produktionsstyrning och trafikstyrning m m. Det rör sig då om datorer som styrmedel inom samhällsområden och funktioner som ofta är störningskänsliga vilket i sin tur medför ett starkt beroende av en fungerande teknik. På grund av att samhället är och blir alltmer genomdatoriserat kommer en mängd verksamheter och företeelser in i bilden vid en diskussion av sårbarheten. Sårbarhetsfrågorna ger en ännu bredare kontaktyta mot samhället än integritetsfrågor. Beträffande dessa finns i alla fall en begränsning till personregisteranvändning.

I SÅRKs utredningsuppdrag ingår att föreslå åtgärder som kan leda

till minskad sårbarhet. Förslag till sådana åtgärder förutsätter givetvis en avvägning mellan olika intressen och strävanden. Det gäller att finna metoder som kan ge önskad effekt utan krångel och onödiga kostnader. Dels gäller det att nå just de områden som är väsentliga från sårbarhetssynpunkt, dels gäller det att för dessa finna lämpligt avvägda åtgärder och insatser. Vilka åtgärder och insatser som sedan bör sättas in är i sin tur avhängigt av vilken verksamhet som är i fråga. SÅRK har pekat på en mängd olika sårbarhetsfaktorer och även angett vilka av dessa som väger tyngst. De olika faktorerna kan emellertid slå olika hårt beroende på verksamheten. Åtgärder som minskar sårbarheten i något avseende kan ibland öka den i ett annat. En sårbarhetsprövning måste därför göras från fall till fall och dessutom vägas mot andra faktorer som ekonomi, effektivitet, integritet m m. Givetvis måste man vara medveten om att det inte går att uppnå någon fullständig säkerhet. Det gäller dock att genom olika åtgärder nå en acceptabel säkerhetsnivå.

Frågan är hur långt man behöver gå när det gäller reglering med hänsyn till de medel som bör sättas in. Ett alternativ är att något organ i samhället får till uppgift att fungera som rådgivande och vägledande i sårbarhetsfrågor. Ett annat är ett heltäckande koncessionsförfarande med rätt att ge olika föreskrifter, kompletterat med tillsynsverksamhet. Ett tredje alternativ kan vara en tillsyns- och rådgivningsfunktion förenad med rätt att ingripa på förekommen anledning. Med detta avses då att om en verksamhet drivs på ett sätt som är oacceptabelt från sårbarhetssynpunkt så skall tillsynsmyndigheten när den får vetskap härom, kunna ingripa med bindande föreskrifter.

En viktig fråga som kommer att diskuteras mer ingående i det följande är om likadana åtgärder krävs på den offentliga och den privata sektorn. Redan nu bör framhållas att de olika alternativen skall ses som utgångspunkt för en diskussion av möjliga lösningar. Detta innebär bl a att en blandning av de olika alternativen kan komma ifråga samt att vissa sektorer kan tänkas bli föremål för mera ingående regleringar än andra. Slutsatsen blir alltså att regleringen och omfattningen av denna även kan variera inom olika områden.

Som SÅRK närmare utvecklat under avsnitt 10.4 har sårbarhetsfrågor beaktats i allt för liten utsträckning hittills. Det är svårt att tro — även om ett ökat medvetande om problemen växer fram — att sårbarhetsaspekterna kommer att beaktas i tillräcklig hög grad och att tillräckligt starka åtgärder kommer att vidtas i framtiden enbart på frivillighetens väg. Visserligen kan upplysning och rådgivning från ett expertorgan bidra till att ett mer långsiktigt och övergripande synsätt på sårbarhetsfrågor anläggs av olika ADB-användare. Frågan är emellertid i vilken omfattning sådana tjänster kommer att tas i anspråk och i vad mån givna råd och anvisningar kommer att följas. Det gäller å andra sidan att inte vidta mer ingripande åtgärder än absolut nödvändigt. I vart fall för vissa användningsområden bör det vara tillfyllest med enbart en rådgivningsfunktion. Det finns för övrigt alltid möjligheter att skärpa eller mildra lagstiftningen efter de behov som framdeles kan uppkomma antingen på grund av samhällets och teknikens utveckling eller enbart på

grund av gjorda erfarenheter. När en sårbarhetsförfattning tillämpats en tid kommer naturligtvis även bedömningsunderlaget att vara betydligt fylligare än det SÅRK nu tagit fram och använt för sina bedömningar.

Om man ser lite närmare på de olika alternativ som nämnts ovan kan följande bedömningar göras. En lösning enligt alternativet med en tillsynsfunktion förenad med rätt att ingripa på förekommen anledning skulle med säkerhet få större genomslagskraft än om enbart en rådgivningsfunktion inrättades. En fördel med ett sådant alternativ skulle dessutom vara att det skulle kräva relativt begränsade insatser på myndighetssidan. Å andra sidan finns nackdelar med en sådan lösning. Bl a skulle den medföra rättsosäkerhet. Vidare finns risk att ingripanden i en del fall skulle komma på ett alltför sent stadium. Vad gäller rättsosäkerheten ligger den i att användarna skulle ha svårt att överblicka och förutse ett ingripande. Någon granskning i form av tillståndsförfarande eller liknande skulle enligt detta alternativ inte ske. Det kan då vara svårt för en datoranvändare att få grepp om vilka krav på åtgärder han förväntas uppfylla för att det skall anses att han löst sina sårbarhetsproblem på ett rimligt sätt. Det är, i vart fall inte för närvarande, möjligt att i lag tillräckligt klart ange vilka krav som användarna skall uppfylla. Något sådant kan möjligen uppnås när ett bättre underlag kommit fram och när man fått viss praktisk erfarenhet av sårbarhetsbedömningar. Detta kan åstadkommas bl a genom att ett tillståndsförfarande införs och används ett antal år. SÅRK bedömer det därför som f n omöjligt att helt komma till rätta med de rättssäkerhetsproblem som sammanhänger med detta alternativ och anser därför att det inte bör komma till användning.

Som SÅRK ovan framhållit kan inte alla sårbarhetsproblem lösas enbart genom rådgivning som sker på frivillig väg även om man med en sådan kan åstadkomma en hel del.

För att komma tillrätta med sårbarhetssituationen, framförallt vad gäller datoranvändning som är av särskild betydelse för samhället, krävs, enligt SÅRKs mening, en omfattande sårbarhetsprövning förenad med möjlighet till bindande föreskrifter. Vad gäller sådana situationer anser SÅRK att det behövs ett tillståndsförfarande. Det bör dock begränsas, bl a med hänsyn till vad som ovan anförts, till att omfatta endast de datoriserade sektorer inom samhället som är av väsentlig betydelse från totalförsvarssynpunkt.

Att införa ett koncessionsförfarande för all ADB-verksamhet med utgångspunkt från sårbarhetsaspekten är för övrigt inte möjligt. En sådan lösning skulle medföra alltför omfattande arbete och kostnader både för tillståndsmyndigheten och datoranvändarna. Någon form av begränsning måste alltså ske. Betydande svårigheter uppkommer emellertid när man skall söka dra gränsen mellan tillståndspliktiga och icke tillståndspliktiga användare. Olika metoder kan användas för att skära bort företeelser som är ointressanta från sårbarhetssynpunkt. En första utgångspunkt bör vara att om möjligt välja ut de områden, som behöver omfattas av ett tillståndsförfarande. Även inom de områden som väljs får man emellertid räkna med att det finns ganska omfattande datoran-

vändning som är utan intresse när det gäller sårbarhetsaspekten. Det gäller då att få bort så mycket som möjligt av sådan användning. Detta kan ske genom t ex generella dispensregler.

Ovan har SÅRK diskuterat olika medel som kan användas för att komma till rätta med sårbarhetssituationen. SÅRK har då i princip kommit fram till att två huvudmetoder skall användas: dels en allsidig sårbarhetsprövning förenad med tillståndstvång, föreskriftsmöjligheter och tillsynsverksamhet för viktigare datoranvändningsområden, dels en rådgivningsverksamhet som skall täcka övriga delar.

Emellertid kan det även finnas behov av någon sorts mellanform, som får omfatta områden som i och för sig är viktiga men ändå inte, av olika skäl, bör falla in under en så långtgående reglering som en tillståndsprövning med åtföljande tillsynsverksamhet. Ett alternativ kan vara ett anmälningsförfarande. Genom ett sådant kan ansvarig myndighet få in material som bl a underlättar en aktiv rådgivningsverksamhet inom områden där sådan rådgivning måste anses som särskilt viktig.

10.5.3 *Formerna för en reglering*

Flera av de åtgärder SÅRK föreslår är av sådant slag att de kräver reglering i lag. Tvingande åtgärder som tillståndsförfarande, bindande föreskrifter och befogenheter att utöva tillsyn förutsätter utan tvekan en lagreglering. Det förefaller ändamålsenligt att samla de mest centrala reglerna om åtgärder för att minska sårbarheten i en särskild lag. SÅRK presenterar ett utkast till en sådan lag med arbetsnamnet sårbarhetslag (SÅRL). Innehållet i SÅRL framgår av bilaga till betänkandet. Syftet med detta utkast är att illustrera SÅRKs förslag till åtgärder i de hänseenden som ovan nämnts. SÅRL upptar även regler om det anmälningsförfarande som föreslås. Den allmänna motiveringen för bestämmelserna i SÅRL redovisas i det följande.

SÅRKs förslag förutsätter även ändringar i myndighetsinstruktioner samt en verkställighetsförordning i anslutning till SÅRL. Utarbetandet av sådana författningar liksom detaljmotivering för de enskilda bestämmelserna i SÅRL bör lämpligen avvakta statsmakternas principiella ställningstagande till de åtgärder SÅRK föreslår.

10.5.4 *Ansvarig datoranvändare*

En grundläggande fråga inom tillstånds- och anmälningsförfarandet är vem som skall åläggas ansvar för att ansökan respektive anmälan sker. Den sålunda ansvarige blir även adressat för eventuella föreskrifter. Vidare förutsätter tillsynsförfarandet vissa skyldigheter för den ansvarige.

Det registeransvarighetsbegrepp som definieras i datalagen är inte lämpligt att använda i detta sammanhang. Ansvaret för sårbarhetsfrågor bör omfatta en vidare krets än den datalagen riktar sig mot eftersom även

annan datoranvändning än den beträffande personregister är aktuell. Datalagens ansvarsbegrepp är inriktat på de enskilda registren medan sårbarhetsprövningen i större utsträckning bör ta sikte på datoranvändarens samlade ADB-verksamhet.

SÅRK anser därför att ansvaret för sårbarhetsfrågorna primärt bör ligga på den som använder datorer som hjälpmedel i sin verksamhet. I de fall vederbörande anlitar servicebyrå är hans möjligheter att påverka sårbarheten i vissa hänseenden beskurna. Ansvaret i dessa delar bör då i stället åvila servicebyrån. I ett följande avsnitt ges en utförligare behandling av frågan om servicebyråernas ansvarighet för sårbarhetsfrågor.

11 Tillståndsförfarande

11.1 Allmänna synpunkter på omfattningen av ett tillståndsförfarande

11.1.1 *Personregister*

SÅRK har pekat på flera sårbarhetsfaktorer som särskilt sammanhänger med personregister. Dels finns problemen med befolkningsregister, dels har SÅRK pekat på betydelsen av register med känslig information. Vidare har SÅRK pekat på att många system med personregister även är funktionellt känsliga. Personregistersidan är även den som är bäst kartlagd genom datainspektionens verksamhet.

Det finns enligt SÅRKs mening skäl att låta personregister — framförallt på den offentliga sidan — omfattas av en sårbarhetsprövning. En prövning av dessa register behöver inte betyda speciellt mycket merarbete för användarna genom att för personregister redan finns ett ansökningsförfarande. För de befintliga system som bör omfattas av en reglering finns på grund härav redan ett omfattande material hos datainspektionen. När det gäller nya system får sådana inte inrättas innan ansökan gjorts hos datainspektionen. Att i en sådan ansökan ta med ytterligare några uppgifter erforderliga för sårbarhetsprövningen bör inte vara alltför betungande för användarna.

11.1.2 *Andra register och användningsområden*

En sårbarhetsprövning enbart av personinformation är inte tillräcklig. Som nämnts finns mängder av annan information av betydelse för sårbarheten. Datorer används emellertid även för andra ändamål än informationsbehandling, nämligen som styrmedel inom samhällsområden och funktioner som ofta är störningskänsliga. Som SÅRK visat i tidigare avsnitt väger sårbarhetsfrågorna ofta lika tungt inom sådana användningsområden. Enligt SÅRKs mening bör därför ett tillståndsförfarande omfatta även delar av dessa.

Vid kartläggningsarbetet har framkommit att sårbarhetsproblem finns såväl inom den statliga och kommunala som inom den privata sektorn. Att undanta någon eller några av dessa områden och lämna dessa helt

utanför ett tillståndsförfarande kan enligt SÅRKs uppfattning inte komma i fråga. Däremot kan tillståndstvång och annan reglering variera i omfattning inom de olika sektorerna.

I följande avsnitt skall SÅRK närmare diskutera omfattningen av tillståndsförfarandet inom de olika sektorerna.

11.2 Tillstånd inom den offentliga sektorn

Till den offentliga sektorn räknar SÅRK alla statliga och kommunala myndigheter inklusive de affärsdrivande verken. Statliga och kommunala bolag är däremot inte inräknade om de inte driver servicebyråverksamhet. Skälet till att servicebyråer skall medräknas skall utvecklas i ett senare avsnitt.

11.2.1 *Försvarsmakten*

Försvarsmakten bör enligt SÅRKs mening undantas från lagens tillämpningsområde. De datorstödda objekten inom det militära försvaret utgörs i första hand av informationssystem för operativ ledning med användningsområde inom högkvarteret och milostaberna och system för taktisk ledning av armé-, marin- och flygstridskrafter. Vidare finns datorstödda system för stridsledning, luftbevakning, flygtrafikledning och vädertjänst. Härutöver har flertalet centrala försvarsmyndigheter ADB-system för sin fredsverksamhet. För dessa system har ÖB det övergripande ansvaret. Bedömning av sårbarhetsfrågor inom denna sektor ingår som en naturlig del i verksamheten. Det finns då ingen anledning att lägga prövningen hos annan myndighet, framförallt inte civil sådan. Samråd bör dock ske mellan ÖB och den civila myndighet, som får huvudansvaret för sårbarhetsfrågor. Framförallt gäller detta ADB-system för fredsverksamheten. Hos ÖB finns redan en omfattande sakkunskap och erfarenhet vad gäller sårbarhetsbedömningar något som bör kunna vara av stort värde i detta sammanhang. Ett ömsesidigt erfarenhetsutbyte bör vara givande för bägge parter.

Begreppet försvarsmakten används i 10 kap 9 § regeringsformen. I förordningen (1975:562) om försvarsmaktens indelning i fred och Sveriges militärterritoriella indelning sägs — och denna avgränsning kan även användas i detta sammanhang — att i försvarsmakten ingår ÖB med försvarsstaben, försvarsgrenarna, försvarsmaktens centrala förvaltningsmyndigheter, försvarsmaktens gemensamma institutioner, utbildningsanstalter och personalkårer samt militärbefälhavarna och chefen för Gotlands militärkommando med staber och förvaltningar. Försvarsmaktens centrala förvaltningsmyndigheter är försvarets civilförvaltning, försvarets sjukvårdsstyrelse, fortifikationsförvaltningen, försvarets materielverk och värnpliktsverket. Till försvarsmaktens gemensamma institutioner räknas försvarets forskningsanstalt, försvarets radioanstalt, försvarets datacentral och krigsarkivet.

11.2.2 *Övriga delar av den offentliga sektorn*

När det gäller övrig datoranvändning inom den offentliga sektorn, förutom den inom försvarsmakten, bör den, enligt SÅRKs mening, i princip underkastas ett tillståndsförfarande. Även lämpligheten av utlandsbearbetningar bör då prövas. Vad SÅRK avser med utlandsbearbetningar skall utvecklas något i det följande.

Ett skäl för ett tillståndsförfarande inom den offentliga sektorn är att inom denna finns många för samhället viktiga system. De är viktiga bl a därför att datorerna används som hjälpmedel för att administrera områden där betydelsefulla åtaganden finns från samhällets sida. Dessa områden kan vara mycket känsliga för störningar. Vidare finns inom myndighetssektorn en stor del av de system som innehåller både bred, djup och känslig information. Genom att en stor del av myndigheternas datoranvändning rör personregister behöver en sårbarhetsprövning inte innebära alltför betungande merarbete för flertalet användare genom att, som nämnts tidigare, en stor del av underlaget för en prövning ändå måste ges in till datainspektionen. Däremot kan naturligtvis föreskrifter som föranleds av prövningen i vissa fall kännas som ett hinder. Det gäller därför att inte meddela andra föreskrifter än som är absolut nödvändiga från sårbarhetssynpunkt.

Ytterligare ett skäl att granska den offentliga sektorn är att många av de offentliga systemen är integrerade med varandra och även med system på den privata sektorn som därigenom många gånger är beroende och styrda av den offentliga ADB-verksamheten.

SÅRK föreslår således som huvudprincip att en tillståndsprövning bör tillämpas generellt för den offentliga sektorn med undantag för försvarsmakten. Denna princip bör emellertid väsentligt modifieras genom att sådan datoranvändning som är ointressant från sårbarhetssynpunkt undantas från prövning. SÅRK återkommer till denna fråga under 11.2.4.

11.2.3 *Sårbarhetsprövningen inom den offentliga sektorn relaterad till vissa övergripande styrmedel*

Inom den offentliga sektorn håller ökade möjligheter att styra ADB-användningen på att införas, främst då på den statliga sidan. Detta förhållande skall beröras något i det följande och då relateras till sårbarhetsfrågorna.

I regeringens proposition 1978/79:121, Användning av ADB i statsförvaltningen, har vissa riktlinjer dragits upp vad gäller den framtida styrningen av datoranvändningen i statsförvaltningen. Som tidigare nämnts skall bl a formella regler utfärdas för etappindelning, beslutspunkter och beslutsunderlag i samband med systeminvesteringar. Reglerna för beslut beträffande större och viktigare investeringar samlas i en särskild handläggningsordning. Affärsverken berörs dock inte av dessa förslag. Vid riksdagsbehandlingen har dessa principer i stort sett godtagits.

Ett av syftena med den föreslagna ordningen är att ansvariga instanser

och personer skall komma in i beslutsprocessen i tillräcklig utsträckning.

Vid behandlingen av propositionen beslutade riksdagen att en datadelegation knuten till regeringskansliet skulle inrättas. Delegationen skall möjliggöra för representanter från riksdagspartier, för arbetsmarknadens parter, kommunförbunden m fl att på ett övergripande sätt kunna följa datafrågorna, inklusive ADB i statsförvaltningen. Delegationen skall även medverka i beredningen av viktigare beslut rörande statlig ADB-verksamhet. Genom delegationen kan även den parlamentariska bevakning av sårbarhets- och säkerhetsfrågor som några motionärer efterlyst, komma till stånd.

Enligt SÅRKs mening behöver denna delegation för att kunna väga in sårbarhetsfrågor i sina bedömningar som får antas vara av övergripande slag, underlag i form av expertutlåtanden av olika slag. En viktig uppgift för det organ som skall ansvara för sårbarhetsfrågor blir att förse delegationen med denna form av material.

En särskild utredare har nyligen sett över organisationen för de centrala myndighetsuppgifterna avseende rationalisering och ADB i statsförvaltningen. Resultatet har redovisats i SOU 1979:72. Utredarens förslag går i korthet ut på att statskontoret i huvudsak behåller nuvarande uppgifter och dessutom får vissa utökade uppgifter på ADB-området. Vidare skall, enligt förslaget, ett råd för granskning av statliga ADB-investeringar inrättas. Den ovan nämnda handläggningsordningen bör enligt utredaren utgöra grund för rådets arbete. Sårbarhetsbedömningar ingår inte bland det föreslagna rådets arbetsuppgifter, såvitt SÅRK kunnat utläsa.

Vid genomförande av nu diskuterade förslag är det enligt SÅRKs mening viktigt att även sårbarhetsfrågorna vägs in i beslutsunderlaget på ett så tidigt stadium som möjligt. Behovet av ett organ som bedömer sårbarhetsfrågor för de statliga systemen finns naturligtvis kvar även vid en mer formaliserad handläggning av ADB-ärenden inom statsförvaltningen. Datadelegationen och granskningsrådet, om det inrättas, ändrar inte denna bild. Bedömning från ansvarigt sårbarhetsorgan får sedan ges i form av yttrande eller bindande beslut beroende på om det är statsmakterna eller någon myndighet som beslutar om ADB-systemets inrättande.

De flesta reformer och lagändringar föregås av offentliga utredningar. I dessa redovisas ibland även förslag rörande användning av ADB-teknik, något som för en del fall även förutsätts i direktiven. Enligt SÅRKs mening bör i förekommande fall i direktiven föreskrivas att i utredningsarbetet skall hänsyn även tas till sårbarhetsfrågor. Härigenom kan sårbarhetsbedömningarna, främst när det gäller statliga system, komma in på ett mycket tidigt stadium.

11.2.4 *Dispensmöjligheter m m*

Som nämnts finns användningsområden inom den offentliga sektorn som är ointressanta från sårbarhetssynpunkt. Det gäller då att finna vägar att undanta sådana tillämpningar från tillståndsplikt.

Vid tillståndsprövningen måste ett ganska fylligt underlag finnas. En komplett ansökan kommer därför att innehålla en lång katalog av uppgifter. Man kan då även tänka sig någon form av förenklat förfarande för mindre viktiga system för vilka man ställer lägre krav på uppgiftslämnande. Vid tillämpningen av datalagen används ett sådant förfarande. Detta innebär att för en del specifierade användningsområden ställs vissa minimikrav. Användare med tillämpningar som faller inom sådana områden och för vilka då även minimikraven är uppfyllda behöver inte ge in en fullständig ansökningshandling utan kan ge in en som endast innehåller ett fåtal uppgifter. Det förenklade förfarandet vid tillämpningen av datalagen gäller i fråga om följande typer av register:

- abonnentregister
- faktureringsregister
- kundregister
- leverantörsregister
- hyresregister
- löneregister
- personalregister
- medlemsregister eller därmed jämställt register.

För bank- och försäkringskundregister gäller ett särskilt förenklat förfarande. Detsamma gäller s k omnibusundersökningar (en sorts statistikregister).

Det förenklade förfarande som används vid tillämpningen av datalagen har visst intresse även när det gäller en sårbarhetslag. Emellertid har flera av de uppräknade registren sitt största användningsområde inom den privata sektorn. Vidare kan en del av dessa register innehålla förteckningar över nyckelpersoner och har då större intresse från sårbarhetssynpunkt än vad gäller integritetsaspekten. Det förenklade förfarande inom datalagens område kan dock ge någon ledning när man försöker finna tillämpningar för vilka någon sorts dispensmöjlighet kan ges enligt en sårbarhetsförfattning.

Genom en nyligen gjord ändring i datalagen har möjligheter införts till generell dispens från tillståndskravet enligt denna lag. Dispensmöjligheten finns intagen i 2 § tredje st datalagen. Den gäller personregister som förs med viss bestämd teknisk utrustning om det med hänsyn till utrustningens art, till utförandet av den automatiska databehandlingen och till registrets utformning i övrigt framstår som uppenbart att otillbörligt intrång i registrerads personliga integritet inte skall uppkomma.

I propositionen med förslag till denna lagändring framhåller föredragande statsråd att mot en sådan generell regel kan invändas att den inte tillräckligt klart anger vilka fall som avses bli undantagna. Slutsatsen blir ändå att en generell regel är den enda möjliga lösningen och som främsta skäl härför anför föredraganden att varje annan lösning med nödvändighet måste bli utomordentligt detaljerad.

Undantaget från tillståndsplikt relateras här som nämnts bl a till den tekniska utrustningen som skall vara av enklare slag. Som exempel på sådan utrustning nämns i förarbetena skrivautomater och andra system

för framställning av text och dokument (s k ordbehandling), datorutrustning för grafisk produktion, kontorsdatorer samt vissa datoriserade konferenssystem, s k telekonferenssystem. Vidare nämns vissa kassaregister inom detaljhandeln. En förutsättning för att undantagsregeln skall vara tillämplig på utrustning av detta slag bör, enligt förarbetena, vidare vara att databehandlingen sker med hjälp av standardprogram eller andra program som endast innebär begränsade bearbetningsmöjligheter.

Kravet på tillstånd och tillståndsansökan enligt datalagen har alltså mjukats upp dels genom det förenklade förfarandet dels genom möjligheten att för vissa fall ge generell dispens då någon ansökan överhuvudtaget inte behöver göras.

När det gäller en sårbarhetsförfattning kan naturligtvis liknande metoder användas. Ytterligare en metod kan vara att ge dispens i det enskilda fallet. Detta skulle då innebära att en datoranvändare som anser att hans tillämpningar är betydelselösa från sårbarhetssynpunkt lämnar en kortare beskrivning av sin datoranvändning till den myndighet som ansvarar för sårbarhetsprövningen. Myndigheten får sedan pröva förutsättningarna för dispens och antingen bifalla eller avslå ansökningen.

Frågan är emellertid om en sådan dispensansökan i någon större utsträckning skiljer sig från ett förenklat förfarande enligt ovan angiven modell. I båda fallen fattas ett beslut; i det ena om tillstånd, i det andra om dispens. Underlagen för besluten kan möjligen variera något men i båda fallen bygger besluten på relativt få uppgifter och prövningen är tämligen summarisk.

Enligt SÅRKs uppfattning bör man om möjligt undvika att ha flera former av undatags- och dispensregler. Ett av skälen härför är att en sådan ordning kan bidra till att göra en sårbarhetsförfattning svårtillämpad och svårtillgänglig framförallt för användarna som får svårt att avgöra vad som gäller för deras fall.

För övrigt är det endast användningsområden som är väsentliga från sårbarhetssynpunkt som bör omfattas av en prövning. Det är samhällets sårbarhet man skall komma till rätta med inte de enskilda systemens. Det kan då ifrågasättas om det finns utrymme för ett förenklat förfarande. Snarare är det så att antingen krävs en fullständig prövning eller också ingen alls.

Slutsatsen blir då att man främst bör sträva efter en generell dispensmöjlighet. Det är naturligtvis svårt att klart ange, liksom i dispensregeln enligt datalagen, vilka fall som avses bli undantagna. En mera detaljerad beskrivning kan emellertid utformas av regeringen eller ansvarig myndighet, inom vissa givna ramar.

Det bör även sägas att vissa former av datoranvändning är av sådant slag att det skulle leda till absurda följder om man ens hävdade att de omfattades av en sårbarhetsförfattning. Som exempel kan nämnas datorer i miniräknare och liknande. Vissa företeelser torde med andra ord helt naturligt falla utanför lagens tillämpningsområde.

När det gäller frågor om dispens bör sådan kunna ges när det är

uppenbart att datoranvändningen inte föranleder några sårbarhetsproblem. Detta kan vara fallet dels när datorer används inom områden där störningar inte ger några effekter på samhället i stort dels när datoranvändningen är av så underordnad betydelse att störningar i datordriften inte medför några allvarligare problem för verksamheten även om den är känslig i sig. Som exempel kan nämnas system som används för en myndighets internadministration och som förhållandevis enkelt kan skötas med andra hjälpmedel. Ytterligare en förutsättning är att det inte rör sig om register med från från sårbarhetssynpunkt känslig information. Även här bör den tekniska utrustningens beskaffenhet tillmätas betydelse. Vidare bör man kunna fästa avseende vid systemstorleken när det gäller dispensprövningen.

Beträffande servicebyråer bör särskilt koncentrationsgraden, typ av bearbetningar och känsligheten hos den information som behandlas tillmätas betydelse vid avgörandet om de skall omfattas av dispens eller ej.

Tidigare har nämnts att det förenklade förfarandet enligt datalagen kan ge viss ledning när det gäller tillämpningen av en dispensregel. Flera av de områden som omfattas av detta förenklade förfarande kan helt eller delvis omfattas av generell dispens när det gäller sårbarhetsprövning. Det kan gälla hyresregister, enklare administrativa register, vissa slags medlemsregister osv.

När det gäller utlandsbearbetningar bör dock alltid en prövning ske och någon dispensmöjlighet således inte finnas. Det utlandsberoende som sådana bearbetningar kan föra med sig och den nya dimension på sårbarhetsproblem som detta beroende ger motiverar en sådan ståndpunkt. Dessutom är det nödvändigt — för prövningsmyndighetens arbete att fortlöpande följa sårbarhetsproblemen — att få en samlad bild av vilken typ av utlandsbearbetningar som förekommer och vilka informationsmängder som förs ut ur landet för att bearbetas och lagras i andra länder.

11.3 Tillstånd inom den privata sektorn

11.3.1 *Allmänna synpunkter*

Till den privata sektorn räknar SÅRK även statliga och kommunala bolag.

Även inom denna sektor finns många olika användningsområden som är av intresse från sårbarhetssynpunkt. Användningssätten är också mera varierande inom denna sektor än inom den offentliga. Ett antal användningsområden är emellertid betydelselösa från sårbarhetssynpunkt. I den mån det uppstår bekymmer med ADB-användningen är det ofta primärt det enskilda företaget som drabbas mera än samhället i stort. På den privata sidan har man dessutom ofta en helt annan ekonomisk press på sig vilket ibland medför ett större intresse för säkerhets- och sårbarhetsfrågor. Ett längre driftavbrott kan många gånger få för-

ödande ekonomiska effekter. Den ekonomiska pressen kan å andra sidan leda till en medveten risktagning då man i stället spar in på åtgärder som kan öka säkerheten och minska sårbarheten.

Det finns vissa områden på den privata sidan som är av väsentlig betydelse för samhället i stort och där det även finns ett starkt beroende av fungerande datorer. Vidare förekommer i vissa fall registerinnehåll som är av betydelse från sårbarhetssynpunkt. När det gäller dessa delar kan det vara nödvändigt att göra mera övergripande och långsiktiga sårbarhetsbedömningar. Det kan då vara motiverat att införa någon form av tvingande reglering.

En stark avgränsning måste dock ske eftersom en obligatorisk reglering av all ADB-verksamhet inom den privata sektorn bl a av anförda skäl och med hänsyn till vad som är praktiskt och ekonomiskt genomförbart knappast kan komma ifråga.

11.3.2 *Tillståndets omfattning*

Utgångspunkten när det gäller den privata sektorn är således att endast vissa avgränsade delar skall omfattas av en tillståndsplikt.

Enligt SÅRKs mening är det främst s k befolkningsregister som även på den privata sidan bör underkastas den mera ingående sårbarhetsprövning som ett tillståndsförfarande innebär. Vidare kan ifrågasättas om inte register med klart avgränsade grupper som är av typ nyckelpersoner bör underkastas en sådan prövning. SÅRK har under 5.1.4 ovan framhållit vilka risker som sammanhänger med sådana register och sådan registerinformation. Där konstateras att de personer en angripare kan tänkas vilja få kontroll över är nyckelpersoner som sedan antingen kan sättas ur spel eller användas för angriparens egna syften. I avsnittet ges även exempel på register som kan innehålla information användbar för sådana ändamål.

Vid tillståndsprövningen av sådana register bör även lämpligheten av utlandsbearbetningar bedömas.

Övriga delar av den privata sektorn och regleringen av dessa behandlas i följande avsnitt.

12 Anmälningsförfarande

12.1 Allmänna synpunkter

Vid ett försök att beskriva återstående delar av den privata sektorn som bör ägnas intresse i förevarande sammanhang och som således inte bör lämnas helt utan reglering, kan en metod vara att ange olika grenar som både är viktiga för samhället i stort och som är starkt beroende av datorer. Inom dessa områden kan sedan närmare bestämmas vilka företag och organisationer som skall omfattas av en reglering.

Den första frågan är hur ingripande denna reglering bör vara. Vissa skäl talar för ett tillståndsförfarande även inom de delar av den privata sektorn som nu angivits. Som nämnts rymmer den för samhället viktiga funktioner med starkt datorberoende och det kan måhända finnas situationer där mer eller mindre tvingande åtgärder kan vara nödvändiga för att man skall komma till rätta med sårbarhetsproblemen. Emellertid torde det, enligt SÅRKs mening, i de flesta fall vara möjligt att på frivillighetens väg, bl a genom råd och anvisningar, komma fram till rimliga lösningar som leder till en acceptabel säkerhets- och skyddsnivå. SÅRK anser det därför inte motiverat att nu föreslå en så långt gående åtgärd som ett tillståndsförfarande. Enligt SÅRKs mening bör man i stället nöja sig med rådgivning och upplysning. För att få ett underlag för denna rådgivningsverksamhet bör dock användarna åläggas en anmälningsplikt. Denna bör omfatta information om bl a maskinell utrustning, dess lokalisering och användningsområde, systemstruktur, säkerhetsåtgärder inklusive katastrofberedskap och typ av registerinnehåll. Möjlighet bör även finnas att vid behov fordra in ytterligare upplysningar. Anmälningsplikten bör även omfatta utlandsbearbetningar. Denna fråga skall behandlas särskilt i det följande. Det material som på detta sätt kommer fram behövs för den fortsatta diskussionen av frågor som rör sårbarhetssituationen i landet samt hur denna skall bemästras.

En omfattande kartläggning av sådant slag kan naturligtvis även bidra till ökad risk för sårbarhet. Vad som avses är att materialet kan komma i orätta händer och användas bl a för att plocka ut lämpliga angreppsmål. Stor varsamhet bör därför iakttagas både vad gäller vilken information som skall tas in och hur denna sedan skall hanteras hos vederbörande myndighet. Även sekretessfrågan måste lösas. Det är för övrigt inte endast det material som skall utgöra underlag för en sårbarhetspröv-

ning som är av intresse i detta sammanhang. Som exempel på andra källor kan nämnas det diarium som idag finns hos datainspektionen och den katalog som statskontorets dokumentationscentral årligen publicerar.

12.2 Det reglerade området

I det följande skall anges några av de delar inom den privata sektorn som är betydelsefulla från sårbarhetssynpunkt.

En gren av intresse är bankväsendet. Som framhållits i lägesrapporten är stora delar av det ekonomiska livet i samhället beroende av att bankernas datasystem fungerar. Avbrott i de datoriserade betalningsströmmarna skulle snabbt medföra stora olägenheter inte bara för bankerna själva utan för samhället i stort.

Även försäkringsbolagen använder sig i stor utsträckning av datorer. Det gäller vid administration av såväl sak- som personförsäkring. Dessa system är känsliga för störningar bl a de delar som rör pensioner och livräntor.

Inom tillverkningsindustrin används datorer alltmer för produktionsstyrning. Detta gäller t ex inom bil-, flygplans- och varvsindustrin. Andra viktiga delar av industrin använder sig av datorer för s k processtyrning. Det gäller t ex järn- och stålverk, pappers- och massaindustri samt petrokemisk industri.

En annan del som är funktionellt känslig är kommunikations- och transportväsendet. Inom denna sektor används datorer i växande omfattning. I vissa fall kan störningar i dessa system ge återverkningar på kommunikationer och transporter som påverkar både näringslivet och den enskilda människan.

När det gäller varuhandeln, har i vart fall de större företagen, i allt större utsträckning börjat använda datorer som hjälpmedel vid distribution och lagerhållning samt ekonomisk redovisning. Störningar i vissa större system inom denna sektor kan ge återverkningar på distributionen och kan bl a medföra varubrist. Det föreligger vidare ett växande beroende mellan detaljhandeln och betalningssystemen hos bankerna.

SÅRK har pekat på koncentrationen som en av de tunga sårbarhetsfaktorerna. Som exempel på funktionell koncentration har angivits bl a det fallet att en mängd kunder vänder sig till en och samma servicebyrå. Problemet ligger då ofta i att en mängd var för sig från sårbarhetssynpunkt mindre intressanta system genom koncentrationen ändå ger en alltför sårbar helhetsbild. Det kan då finnas ett behov av att i första hand ge anvisningar och råd till den — det kan vara en servicebyrå eller något annat företag — som åtagit sig datordriften för andra.

Här har endast vissa viktiga sektorer inom den privata sektorn av intresse från sårbarhetssynpunkt angivits. Alla företag och organisationer inom dessa sektorer är naturligtvis inte intressanta vid sårbarhetsbedömningar. Många företag är av den storleken att de har ringa betydelse för samhället i stort. Vissa företags användning av datorer kan

vara av så underordnad betydelse för företagets verksamhet att det i realiteten inte föreligger något beroende av denna teknik.

För att fånga de företag och organisationer som är av intresse i förevarande sammanhang och för att lämna övriga utanför en reglering bör möjlighet finnas att förordna om vilka företag och organisationer som inom nu nämnda sektorer bör omfattas av anmälningsplikt.

En väg att nå intressanta områden och företag är att utgå från de s k K-företagen. Dessa företag finns förtecknade hos ÖEF. Registret förs med stöd av ett kungligt brev från den 24 mars 1949 och skall innehålla de företag, vilkas verksamhet ÖEF finner vara av särskild betydelse för att tillgodose landets behov av förnödenheter och tjänster under krig.

K-företagen finns i stort sett inom de områden som ovan angivits som betydelsefulla från sårbarhetssynpunkt. Dessa företag har dessutom bedömts som viktiga för landet i krislägen, och torde ganska väl motsvara dem SÅRK anser vara av intresse från sårbarhetssynpunkt. K-företagen uppgår i dag till 12 — 13 000. Alla är dock inte datoranvändare. Vidare kan man anta att en del av K-företagens ADB-användning är av underordnad betydelse något som för de flesta fall gör dem ointressanta från sårbarhetssynpunkt. SÅRK anser dock att K-företagen kan tas som utgångspunkt för att bestämma det område som bör omfattas av en reglering och föreslår att man låter K-företag som använder datorer, dock med vissa undantag, omfattas av en anmälningsplikt. Eftersom dessa företag redan finns förtecknade och redan är föremål för viss myndighetsutövning är det praktiskt att använda denna urvalsmetod.

Det är naturligtvis svårt att nu finna exakt de områden som bör regleras och hur ingripande regleringen bör vara. Den nu valda metoden bör dock kunna vara användbar för en grundläggande reglering. På ett senare stadium får man vara beredd att göra olika justeringar. En översyn av lagen kommer i vilket fall som helst att bli erforderlig sedan den varit i kraft en tid dels på grund av den snabba utvecklingen inom detta område dels med hänsyn till de erfarenheter som lagen i praktisk tillämpning kommer att ge.

12.3 Utlandsbearbetningar och lagring av information utomlands

En särskild fråga är i vad mån utlandsbearbetningar skall underkastas en generell granskning även på den privata sidan. Först skall något diskuteras vad som avses med utlandsbearbetningar. I detta begrepp innefattar SÅRK situationer där svensk information finns i eller förs över till utlandet och bearbetas där för att sedan i bearbetat skick föras tillbaka till Sverige. Det kan även finnas skäl att intressera sig för fall då lagring av svensk information sker utomlands även om den inte bearbetas utanför våra gränser. Däremot avses inte fall som innebär ren transport av data över gränserna t ex av den typ som SWIFT-systemet innebär eller när information hämtas från utländska databanker till Sverige.

I tidigare avsnitt har SÅRK pekat på att det inom den privata sektorn

förekommer internationellt dataflöde inom de flesta verksamheter — vilket ibland även innebär bearbetningar utomlands. SÅRK har även påpekat att flera servicebyråer i Sverige förmedlar tjänster som innebär bearbetningar utomlands. Vidare har SÅRK uttalat att det ökade dataflödet över gränserna medför säkerhets- och sårbarhetsproblem av andra dimensioner än de som finns om man endast ser på rent nationella förehållanden och att det är svårare att skydda sig mot händelser utom riket än att bygga upp ett inhemskt skydd.

Frågan är om denna ytterligare dimension på problemen bör medföra en granskning även av områden som inte i övrigt skall omfattas av tillstånds- eller anmälningsplikt. Enligt SÅRKs mening bör detta inte ske. Skälet härför är främst att ett tillräckligt underlag vad gäller frekvens och typ av bearbetningar inte finns för att avgöra i vad mån en sådan reglering har fog för sig. Däremot bör en djupare kartläggning göras inom detta område och det kan lämpligen ske genom att frågan om utlandsbearbetningar särskilt uppmärksammas vid det tillstånds- och anmälningsförfarande som ovan föreslagits.

Det material beträffande utlandsbearbetningar som på detta sätt kommer in måste naturligtvis bearbetas på lämpligt sätt bl a för att kunna tjäna som underlag för rådgivningsverksamhet. Materialet kan även tjäna det syftet att statsmakterna före en kris har tillgång till ett underlag som ger möjligheter att överblicka i vad mån och i vilken omfattning utlandsbearbetningar sker. Materialet bör som antytts, även kunna användas som underlag för vidare diskussion av frågan om tillståndsplikt framdeles bör införas.

Avslutningsvis vill SÅRK framhålla att reglering inom detta område bör ske med viss försiktighet bl a med tanke på det värde som ligger i internationellt utbyte av olika slag. Å andra sidan kan man förmodligen räkna med en viss restriktiv reglering i andra länder och frågan är om det inte inom detta område på sikt föreligger behov av internationella överenskommelser.

SÅRK har nu angett områdena för tillstånds- och anmälningsplikt. Som kommer att utvecklas närmare i det följande lägger SÅRK stor vikt vid informations- och rådgivningsverksamheten. Anmälningsplikten har även till viss del motiverats med att den skall ge bättre underlag för rådgivningsverksamhet. Det kan redan nu nämnas att rådgivningsverksamheten förutsätts omfatta även delar som varken omfattas av tillstånds- eller anmälningspolikt. Som nämnts kommer rådgivning och informationsverksamhet att behandlas utförligare i ett senare avsnitt.

13 Dataservicebyråverksamhet

Som SÅRK tidigare framhållit bör även servicebyråer omfattas av en sårbarhetsförfattning och ha ett ansvar enligt denna. Flera skäl härför kan anföras. SÅRK har funnit koncentrationen vara en av de tyngre sårbarhetsfaktorerna. Som ett exempel på funktionell koncentration har SÅRK bl a nämnt det fallet att en mängd kunder vänder sig till en och samma servicebyrå. Det föreligger alltså ett behov av att kunna rikta föreskrifter även mot servicebyråer i syfte att minska den sårbarhet som koncentrationen kan föra med sig.

Många gånger kan naturligtvis servicebyråer påverkas indirekt i samband med prövning av själva systemen. Man kan t ex neka en användare med från sårbarhetssynpunkt känsliga tillämpningar att anlita viss servicebyrå om den inte anses motsvara de krav som bör ställas.

I vissa fall kan det emellertid vara så att flertalet av de enskilda systemen inte är speciellt känsliga och således inte motiverar sådana åtgärder. Ändå kan mängden system, alltså koncentrationen, göra en sådan servicebyråverksamhet känslig.

Det kan många gånger vara svårt för kunderna hos en servicebyrå att genom byrån få det underlag om datordriften som behövs för en sårbarhetsprövning. Det kan även vara svårt för att inte säga omöjligt för kunden att i full utsträckning påverka datordriftens utseende eller att få ett grepp om hur de krav på säkerhet m m som han ställer uppfylls.

SÅRK anser bl a med hänsyn till vad som nu anförts att det inte kan anses tillräckligt att — i vart fall gäller detta större och viktigare servicebyråer — insynen i och möjligheterna att påverka servicebyråernas verksamhet endast kan ske indirekt genom kunderna. Enligt SÅRKs mening bör därför även vissa servicebyråer omfattas av tillstånds- eller anmälningsplikt. Den ansvariga myndigheten kan härigenom få ordentlig inblick i verksamheten och i vissa fall även möjlighet att ge erforderliga föreskrifter om hur denna får drivas.

Begreppet servicebyrå är inte entydigt. Det finns företag som renodlat ställer datorkraft och därtill hörande tjänster till förfogande och då alltså inte driver någon egen verksamhet där datorerna används som hjälpmedel. Vidare finns företag som använder datorer i den egna verksamheten men som säljer eventuell överkapacitet. I vissa fall har man inom koncerner skapat en egen servicebyrå som alltså är ett fristående företag, som helt eller delvis sköter övriga koncernföretags datordrift. I vissa fall

tillhandahålls endast vissa tjänster t ex hjälp med överföring av information till ADB-medium.

Vad SÅRK avser med servicebyråverksamhet är användning av datorer med därtill hörande tjänster för annans räkning när detta sker i mer betydande omfattning och när det sker kontinuerligt och alltså inte är av mera tillfällig karaktär. Ren dataregistreringsverksamhet inräknas inte i begreppet.

Ovan har beskrivits vad en sårbarhetslag skall omfatta inom olika sektorer. Samma utgångspunkt bör givetvis gälla för servicebyråsidan. SÅRK har dock ansett att när det gäller servicebyråer inom den offentliga sektorn bör dessa bli föremål för ett tillståndsförfarande oavsett om de bedrivs i myndighets- eller bolagsform. Skälet härför är att prövningen inom den offentliga sektorn har ansetts som särskild viktig. Den bör då även gälla om själva datordriften är förlagd till ett statligt eller kommunalt bolag. Vid en annan ordning skulle t ex Kommundata AB på sin höjd omfattas av ett anmälningsförfarande.

SÅRK anser att i övrigt kan huvudmodellen följas. Detta innebär anmälningsplikt för vissa servicebyråer som är K-företag enligt tidigare beskrivning samt rådgivningsverksamhet för övriga delar.

Ett problem som kan uppstå enligt nu skisserad lösning är att när offentliga användare anlitar privata servicebyråer, som då alltså inte är tillståndspliktiga, kommer ändå inte någon ingående granskning att kunna göras annat än på frivillighetens väg. I de fall det gäller en anmälningspliktig servicebyrå får man då, om det rör sig om känsliga system förbjuda användaren att vända sig till sådan byrå om inte byrån är beredd att till alla delar medverka till att sårbarhetsproblemen löses på ett godtagbart sätt. Vad därefter gäller servicebyråer som inte är underkastade tillstånds- eller anmälningsplikt får förutsättas att datoranvändaren så långt som möjligt verkar för att anlitad servicebyrå uppfyller rimliga krav i fråga om säkerhet.

Ett annat problem som sammanhänger med att servicebyråer på den offentliga och privata sidan behandlas olika är att en sådan ordning kan medföra att konkurrens inte kan ske på lika villkor. För att motverka sådana inte önskade effekter måste ansvarig myndighet vara mycket försiktig innan kostnadskrävande åtgärder föreskrivs.

Ovan har anmärkts att vid tillståndsprövning av olika system kan en användare nekas att anlita en viss servicebyrå om byrån inte är beredd att medverka till lösningen av sårbarhetsproblem. Vid en sådan situation bör naturligtvis samma höga krav ställas som om det gällde en tillståndspliktig byrå. Härigenom kan även en sned konkurrenssituation motverkas.

Granskningen av servicebyråer får göras med utgångspunkt bl a från de system som drivs hos servicebyrån. Detta innebär att ett godkännande inte kan gälla för någon längre tid utan omprövning måste ske då och då med tanke på förändringar i driften bl a genom att nya system tillkommer.

En granskning av servicebyråer kan vidare endast omfatta de punkter som en servicebyrå har ett naturligt ansvar för. Dessa punkter har angetts

i ett tidigare avsnitt. Det naturliga ansvarsområdet begränsar även föreskriftmöjligheterna som givetvis endast kan gälla de områden en servicebyrå råder över. Servicebyråernas ställning i detta avseende skall beröras i samband med behandlingen av vilka olika möjligheter till föreskrifter som överhuvudtaget bör finnas.

Även när det gäller servicebyråer bör dispensmöjligheter finnas. Vad som bör undantas är mindre byråer som dessutom inte har några känsliga system i drift.

14 Övergångsbestämmelser

Enligt SÅRKs mening finns starka skäl att i första hand inrikta tillstånds- och anmälningsplikten på nya system och tillämpningar eller på system och tillämpningar som undergår väsentliga förändringar. Ett sådant förslag kan tyckas rimma illa med vad SÅRK uttalat om rådande sårbarhetssituation. Med tanke på kostnader, resurser och möjliga effekter är det ändå, enligt SÅRKs mening, lämpligt att välja denna ambitionsnivå. Ett tillstånds- och anmälningsförfarande beträffande alla befintliga system och andra användningsområden skulle betyda ett mycket stort antal ärenden med åtföljande arbete för användare och tillståndsmyndighet. Naturligtvis skulle sårbarheten genom ett sådant förfarande minskas i vissa avseenden. Frågan är emellertid om arbetsinsatsen står i rimlig proportion till de positiva effekter som man skulle uppnå. Ett skäl till tveksamhet är att en sårbarhetsprövning ändå många gånger inte skulle medföra önskat resultat på grund av de svårigheter och kostnader som väsentliga ändringar i befintliga system skulle föra med sig. Det är ofta så att vissa säkerhets och andra åtgärder som leder till minskad sårbarhet måste planeras in och vidtas redan från början för att ge önskad effekt. Detta innebär med andra ord att åtgärder som vidtas på ett stadium när systemen redan är färdiga ofta kan medföra betydande merkostnader.

Det finns å andra sidan en hel del åtgärder som kan vidtas beträffande befintliga system utan att de medför sådana merkostnader. Det kan t ex gälla olika reservrutiner, katastrofplaner och katastrofberedskap, personalplanering, användning av kryptering m m. Det är naturligtvis angeläget att alla rimliga åtgärder som kan minska sårbarheten vidtas beträffande befintliga system.

Redan det faktum att sårbarhetsfrågorna har börjat uppmärksammas och diskuteras kommer med stor säkerhet att medföra förbättringar. Den myndighet som skall handha sårbarhetsfrågor måste även bidra med en aktiv rådgivningsverksamhet och därigenom bidra till en gynnsam utveckling även vad gäller befintliga system.

Enligt SÅRKs förslag skall tvingande åtgärder i huvudsak sättas in på den offentliga sektorn. Den myndighet som ansvarar för sårbarhetsfrågor är naturligtivs oförhindrad att ta upp diskussioner med olika myndigheter och påtala eventuella brister även i befintliga system. Eftersom det i regel ligger i myndigheternas eget intresse att avhjälpa sådana

brister kan man ändå nå betydande förbättringar vad gäller sårbarhetssituationen. När det gäller statliga myndigheter kan dessutom tillståndsmyndigheten — om inte förbättringar kan uppnås på annat sätt — uppmärksamma regeringen på företeelser som inte är godtagbara från sårbarhetssynpunkt. Regeringen kan därefter vidta lämpliga och erforderliga åtgärder bl a i samband med budgetarbetet.

Slutsatsen blir alltså att de mera långtgående åtgärderna för att motverka sårbarheten skall sättas in beträffande nyinrättade system och nya användare samt när befintliga system underkastas väsentliga förändringar. Detta gäller då även den anmälningsplikt som föreslagits omfatta vissa delar av den privata sektorn.

Frågan är emellertid om befintliga tillämpningar helt skall lämnas utanför den tvingande regleringen eller om även dessa skall prövas efter viss övergångstid. Om man lämnar de befintliga systemen helt utanför kan det finnas risk att vissa tillämpningar inte kommer att underkastas sårbarhetsprövning genom att endast smärre förändringar successivt görs. Det kan då hävdas att väsentliga förändringar inte sker. Det kan även tänkas att en tillämpning kan låsas fast under en längre tid. Härigenom skulle strävanden att minska sårbarheten motverkas. Om det finns en kontrollpunkt i framtiden kan detta även ses som en markering av att olika användare under övergångstiden bör — i den mån det är rimligt — vidta åtgärder som bidrar till minskad sårbarhet. Vid övergångstidens slut, när alltså en prövning skall ske, ökar möjligheterna för de användare som fortlöpande försökt anpassa sig till de krav en sårbarhetsförfattning ställer, att fortsätta driften utan att några större omvälvningar behöver ske. Det bör dock även sägas att lika höga krav i regel inte kan ställas på äldre tillämpning som på nya sådana.

Av nu anförda skäl föreslår SÅRK att en tillståndsprövning sker även av befintliga system efter en viss övergångstid. Denna kan lämpligen utsträckas till fem år.

15 Innebörden av tillståndsförfarandet

15.1 Grundläggande regler

SÅRK föreslår alltså ett tillståndsförfarande inom vissa angivna områden. Lämplig tillstånds- och tillsynsmyndighet kommer att diskuteras i ett senare avsnitt. Innebörden av ett tillståndsförfarande blir att berörda system underkastas en allsidig sårbarhetsprövning med möjligheter till bindande föreskrifter. Ytterst — något som måste ses som rena undantagsfall — kan tillstånd vägras.

När det gäller ADB-användning som beslutats av regering och riksdag kan det inte bli fråga om någon tillståndsprövning. Sådana system bör dock underkastas en lika noggrann granskning som sedan får ligga till grund för yttrande till statsmakterna. Ett beslut från statsmakterna om ADB-användning bör alltså föregås av ett yttrande från den myndighet som ansvarar för sårbarhetsfrågorna. Myndigheten bör även ges rätt att ge bindande föreskrifter i den mån sådana inte givits av statsmakterna.

15.2 Förutsättningar för att meddela tillstånd

Om datoranvändningen, med de eventuella föreskrifter som ges, kan ske på en från sårbarhetssynpunkt acceptabel nivå skall alltså tillstånd meddelas.

Att göra något skarp och detaljerad beskrivning av vad som kan anses som acceptabelt från sårbarhetssynpunkt är omöjligt. Det måste bli en bedömning från fall till fall där olika sårbarhetsfaktorer och även andra faktorer vägs mot varandra. Praxis kommer att få ge begreppet ett närmare innehåll men riktmärken och linjer måste dock ges i lagstiftningen och i dess förarbeten.

SÅRK har i tidigare avsnitt tagit fram olika sårbarhetsfaktorer. Som de mest betydande av dessa har SÅRK bedömt utlandsberoende, koncentrationsproblem, personalberoende samt risker förknippade med vissa typer av registerinnehåll. Samtliga faktorer får tas som utgångspunkt när ett system eller användningsområde granskas. Olika faktorer kan då väga olika tungt beroende på verksamhetens art. Vad som kan anses som acceptabelt från sårbarhetssynpunkt får sedan vägas mot hur störningskänslig och hur samhällsviktig verksamhet det är frågan om eller hur känslig information som behandlas. Som nämnts måste dessutom andra faktorer som rationalitet, ekonomi, integritet m m vägas in

i bilden. Den fackmyndighet som skall ägna sig åt sårbarhetsfrågorna får naturligtvis koncentrera sig på dessa. Bedömningar av rationalitet och ekonomi etc måste i första hand vara en fråga för användarna och något som sårbarhetsmyndigheten inte primärt bör befatta sig med. Å andra sidan kan denna myndighet inte helt bortse från sådana aspekter när olika föreskrifter skall ges. Som närmare kommer att utvecklas i det följande bör besvärsprövningen ligga hos regeringen. Vid denna prövning finns — och detta är huvudskälet till att regeringen bör handha denna — större utrymme för att väga olika intressen mot varandra.

Det är naturligtvis ofta flera sårbarhetsfaktorer som kan verka på samma system och ge en sammantagen effekt som gör sårbarheten högre än om endast en faktor skulle spela in. Ibland kan det också vara så att låg sårbarhet relaterad till en faktor kan innebära hög sårbarhet i annat avseende. Som exempel kan nämnas att decentraliserade lösningar kan minska följderna av olika slags angrepp men kan även i vissa fall ge ett ökat personalberoende och beroende av fungerande datakommunikationer.

Några exempel på situationer vid vilka sårbarhetsnivån inte nått en acceptabel eller tillräckligt låg nivå skall ges i det följande.

När det gäller befolkningsregister har i lägesrapporten påtalats de risker som är förknippade med dessa. Ett övergripande mål bör därför vara att i görligaste mån begränsa spridningen av sådana register. Vissa befolkningsregister kommer likafullt att finnas kvar. När det gäller dessa kan en för hög sårbarhet ligga i att skyddsnivån inte är tillfredsställande med bl a risk för att kopior alltför lätt kommer i orätta händer eller i att planeringen för undanförsel och förstöring är för dålig. Liknande problem kan finnas beträffande register med känslig information av olika slag. Ju känsligare information desto större krav måste ställas på säkerhet i olika avseenden bl a användning av kryptering och olika behörighetskontroller.

Som SÅRK påpekat bl a i kapitel 10 föreligger ofta stor sårbarhet hos de stora centrala systemen och dataanläggningarna till vilka även räknas de stora servicebyråerna. De är i princip utsatta för flertalet av de risker SÅRK pekat på vid sin kartläggning. För att motverka dessa svagheter bör utgångspunkten vara att sprida driften av systemen men att utveckla system centralt. Härvid bör speciellt möjligheten att utnyttja distribuerad databehandling särskilt undersökas, eftersom denna teknik underlättar central utveckling och centralt underhåll av system där driften är geografiskt spridd. Den distribuerade databehandlingen kan även minska sårbarheten genom att dubbellagring av information i lokala och centrala register kan åstadkommas på ett kontrollerat och rationellt sätt. Härigenom skapas möjligheter bl a att rekonstruera data. Ibland kan naturligtvis centrala driftlösningar av olika skäl vara att föredra. Stora krav måste då ofta även ställas på säkerhet, dokumentation, back-up, katastrofberedskap etc för att systemet skall kunna godtas från sårbarhetssynpunkt.

Vid tillståndsprövningen bör även en strävan vara att motverka den geografiska koncentrationen.

Utlandsberoendet är en viktig sårbarhetsfaktor som uppträder i olika former. Det beroende som ligger i behovet av datorer, komponenter, reservdelar, service etc från utlandet är av stor vikt och kanske det som är svårast att komma till rätta med. Det är knappast problem som kan ges tillfredsställande lösningar genom föreskrifter i ett tillståndsärende. Som faktor bör dock denna form av utlandsberoende vägas in vid en allmän sårbarhetsbedömning och en del åtgärder — varom mer i det följande — kan även vidtas. När det gäller den form av beroende som uppstår genom bearbetningar utomlands ligger sårbarheten här bl a i en ökad risk för att känslig information skall komma i orätta händer. Vidare kan det vid bearbetningar utomlands uppstå problem med att återfå informationen och ordna back-up rutiner. Överhuvudtaget kan det vara svårt att skydda sig mot olika händelser utom riket. Beträffande funktionellt eller innehållsmässigt mycket känsliga system bör därför övervägas i vad mån utlandsbearbetningar över huvud taget bör tillåtas. Denna form av utlandsberoende kan alltså motverkas i samband med ett tillståndsförfarande.

När det gäller beroendet av nyckelpersoner är även detta en av de tunga sårbarhetsfaktorerna. Detta beroende förstärks om det rör sig om komplicerade system som dessutom har bristfällig dokumentation. Det rör sig här om flera sårbarhetsfaktorer som var och en för sig kan vara av allvarlig natur men som framförallt i kombination kan medföra alltför hög sårbarhet.

De tyngsta sårbarhetsfaktorerna har nu behandlats och det är av naturliga skäl främst dessa som särskilt bör beaktas vid sårbarhetsprövningen. Sårbarheten förstärks ytterligare av flertalet andra faktorer som SÅRK pekat på vid sitt kartläggningsarbete. Det kan gälla bristfällig dokumentation, brister i säkerhetsarbetet, bristande planering, bl a katastrofplanering, bristfällig utbildning och kunskap hos datoranvändarna, brist på standardisering etc.

En viktig utgångspunkt vid sårbarhetsprövningen bör vara att hela tiden ha som mål att endast fånga upp verksamheter som har betydelse för samhället i stort och att inom dessa sektorer uteslutande ägna sig åt företeelser som kan innebära allvarligare störningar, hot eller risker. I ett tillståndsärende får de olika sårbarhetsfaktorernas inverkan bedömas och i möjligaste mån motverkas med föreskrifter. Om med de föreskrifter som meddelas ett system kan antas hamna på en acceptabel säkerhetsnivå skall tillstånd meddelas.

Det kan för vissa situationer finnas skäl att ge tillstånd endast för viss begränsad tid. Det kan t ex gälla system som är särskilt känsliga från sårbarhetssynpunkt och därför kan behöva omprövas efter viss tid.

15.3 Bindande föreskrifter

I tidigare avsnitt har angivits vad en sårbarhetsprövning bör omfatta. I anslutning till denna prövning bör även vid behov bindande föreskrifter kunna meddelas.

15.3.1 *Registerinnehåll*

När det gäller registerinnehåll bör finnas en möjlighet att ge föreskrifter om vilka uppgifter som får ingå i ett register. Vid en prövning av arten, mängden — och när det gäller befolkningsregister — personkretsen kan det från sårbarhetssynpunkt finnas ett behov av att ge föreskrift om ett gentemot ansökningen modifierat innehåll. En föreskrift om innehållet gör det även möjligt att följa ev ändringar eftersom sådana förutsätter nytt tillstånd.

Möjligheter bör även finnas att föreskriva om vilka bearbetningar som får göras, vilka uppgifter som får göras tillgängliga, om utlämnande och annan användning samt om bevarande och gallring.

När det gäller befolkningsregister och register med känslig information bör som nämnts även prövas att planläggningen för undanförsel och förstöring är tillfredsställande ordnad. Detta är en fråga som närmast berör ÖEFs verksamhet. Den kännedom och överblick som tillståndsförfarandet kommer att ge bör ge ett gott underlag för sådan planering. Oavsett vilken myndighet som skall ha huvudansvaret för sårbarhetsfrågorna bör dock föreskrifter i detta avseende även fortsättningsvis ges av ÖEF som därvid bör samråda med ansvarig myndighet och utnyttja det underlag som kan finnas hos denna.

15.3.2 *Koncentration*

Som ett medel att motverka den geografiska och funktionella koncentrationen bör även möjligheter finnas att ge föreskrift om datordriftens organisation. Att komma till rätta med den geografiska koncentrationen måste dock i mycket ske med andra medel. När det gäller statliga myndigheter får mera övergripande långsiktiga lokaliseringsåtgärder ankomma på i första hand statsmakterna. Frågan om datorernas lokalisering hänger ju till stor del ihop med var den verksamhet som skall använda datorerna är belägen.

För att motverka den funktionella koncentrationen kan det ibland vara befogat att ge föreskrifter av bindande karaktär. Naturligtvis måste detta ske med försiktighet varvid även andra faktorer måste beaktas, som ekonomi, rationalitet, behov av att snabbt få riksomfattande information, datakommunikationslösningar etc. En allmän utgångspunkt bör som nämnts vara att driften om möjligt skall spridas och att möjligheterna att utnyttja distribuerad databehandling därvid skall undersökas. Härigenom kan man även få vissa effekter som bidrar till att minska den geografiska koncentrationen.

15.3.3 *ADB-säkerhet*

Som ett led i att motverka olika angrepp utifrån måste även ingå möjlighet att ge föreskrifter om fysiskt skydd. Med detta avses enligt gängse terminologi skydd mot

— obehörigt tillträde
— brand

— vatten och annan vätskeuttömning
— långvariga avbrott i försörjningssystem (el-, vatten- och klimatförsörjning)
— övriga störningar (bl a elektromagnetisk strålning).

Vidare bör möjlighet till föreskrifter finnas som rör dataskydd bl a då föreskrifter om skydd genom behörighetssystemen och användning av kryptering etc samt föreskrifter som rör funktionsskydd för att komma till rätta med brister i maskin- och programvara, samt föreskrifter som rör kvalitetsskydd av data. Olika säkerhetshandböcker bl a de som utarbetats av statskontoret bör kunna vara vägledande när föreskrifter beträffande olika skyddsåtgärder skall ges.

15.3.4 *Personalberoende, dokumentation m m*

Om det visar sig att personalberoendet är en påtaglig sårbarhetsrisk bör även föreskrifter kunna meddelas om åtgärder som minskar detta beroende. Det kan innebära krav på att fler personer anställs eller att personal som finns får en bredare utbildning och ett bredare ansvarsområde. När det gäller personalberoendet kommer även värnpliktsförhållandena (jfr 18.4) in i bilden. Personalberoendet kan förstärkas om dokumentationen är bristfällig. Bristfällig dokumentation är även en sårbarhetsfaktor i sig. Föreskrifter om dokumentation skall därför även kunna meddelas. Dokumentationen bör vara i sådant skick att den möjliggör en total rekonstruktion. Detta innebär bl a att dokumentationen måste hållas aktuell.

15.3.5 *Integration och inbördes beroende*

Beroendet av andra system kan som tidigare påpekats medföra sårbarhetsproblem. För vissa situationer kan det därför finnas behov av att ge föreskrifter om i vilken utsträckning samkörning och integrering mellan olika system kan godtas. Vad man framförallt bör förebygga med sådana föreskrifter är dels komplicerade och därmed sårbara knytningar mellan olika viktiga system dels att datoranvändare inom viktiga sektorer har svårt att kontrollera den egna verksamheten genom ett starkt externberoende.

15.3.6 *Katastrofberedskap*

Mycket arbete och möda har lagts ner på olika förebyggande åtgärder som alltså skall förhindra att oönskade händelser inträffar. En minst lika viktig del som blivit något försummad är planer och rutiner som kan sättas in om — trots alla försiktighetsåtgärder — en katastrof inträffar.

Tillståndsmyndigheten bör därför lägga stor vikt vid att olika maskinella och manuella reservrutiner finns samt ges möjlighet att meddela föreskrifter i detta hänseende. Det räcker emellertid inte med att reservrutiner finns. Det krävs även att det för olika katastrof- och beredskapslägen finns väl genomtänkta och även prövade planer. Stor uppmärk-

samhet bör alltså ägnas katastrofberedskap och katastrofplanering och även i detta hänseende bör tillståndsmyndigheten ha möjlighet att meddela bindande föreskrifter. Sådana planer kan för övrigt bidra till att spara in på diverse, ofta kostsamma, förebyggande säkerhetsåtgärder. Vet man att verksamheten kan fungera hjälpligt även om allvarligare händelser inträffar är sådana förebyggande åtgärder inte lika starkt motiverade.

15.3.7 *Utlandsbearbetningar*

När det gäller de tillståndspliktiga systemen bör en bedömning även göras om utlandsbearbetningar lämpligen bör ske. Föreskrift om att sådana, helt eller delvis, inte får förekomma bör då också kunna meddelas. Av skäl som tidigare angivits bör man dock iaktta en viss återhållsamhet när det gäller förbud mot utlandsbearbetningar. I vissa fall kanske sårbarhetsproblemen kan lösas på andra sätt t ex genom föreskrifter om olika reservrutiner inom landet. Det kan t ex gälla krav på att reservbearbetningskraft skall finnas inom landet.

15.3.8 *Föreskrifter vad gäller servicebyråer*

Vad gäller servicebyråer skall föreskriftsmöjligheterna beträffande den rena servicebyråverksamheten omfatta

- ADB-säkerhet
- åtgärder som motverkar personalberoende
- dokumentation
- katastrofberedskap
- utlandsbearbetningar.

15.3.9 *Föreskrifter vad gäller system om vars inrättande statsmakterna beslutat*

Myndigheten bör även vara skyldig att meddela föreskrifter beträffande system om vars inrättande statsmakterna har beslutat. Detta gäller i den mån statsmakterna inte har meddelat föreskrift i samma hänseende.

15.3.10 *Föreskrifter i samband med tillsynsverksamheten*

För att följa utvecklingen och för att kontrollera att tillstånd och föreskrifter följs bör tillståndsmyndigheten även ges en tillsynsfunktion. Tillsynsverksamheten skall behandlas närmare i det följande. Om det vid tillsynen framkommer att meddelade föreskrifter inte är tillräckliga eller att tillstånd inte borde ha givits bör myndigheten ha möjlighet att ingripa och ge ändrade föreskrifter eller — i sista hand — återkalla meddelat tillstånd.

Tillsynen bör även omfatta sådana system som beslutats av statsmakterna och även när det gäller dessa skall myndigheten kunna gå in och meddela ändrade föreskrifter i den mån dessa inte strider mot statsmakternas beslut. Skulle en sådan situation uppstå som kräver åt-

gärder från någon av statsmakterna bör det åligga myndigheten att göra anmälan om detta.

15.3.11 *Åtgärder när driften av system upphört*

När det gäller befolkningsregister och register med känslig information som inte längre skall föras bör det finnas möjligheter att föreskriva hur det skall förfaras med registren. För att förebygga risk att informationen hamnar i orätta händer kan det t ex finnas skäl att föreskriva att registren förstörs eller gallras. Samråd bör då även ske med riksarkivet.

15.4 Straffsanktioner

I syfte att så god efterlevnad som möjligt skall uppnås bör även straffbestämmelser införas. Straff bör alltså föreskrivas för den som använder tillståndspliktiga system utan tillstånd, för den som inte fullgör sin anmälningsplikt och för den som bryter mot meddelade föreskrifter. Vidare bör även den som lämnar osanna uppgifter i samband med tillståndsansökningen eller i anmälan eller i samband med att sårbarhetsmyndigheten begär uppgifter och upplysningar vid sin tillsynsverksamhet, kunna straffas.

Vid grövre överträdelser av lagens bestämmelser som tillika medför allvarliga sårbarhetsrisker bör möjligheter även finnas att förverka datorutrustning, programvara och register. Förverkande torde i huvudsak kunna ifrågakomma när känslig information registreras utan tillstånd eller på sätt som strider mot givna föreskrifter.

En förverkanderegel torde få relativt liten praktisk betydelse. En sådan möjlighet bör dock finnas. I samband med tillsynsverksamheten bör även möjligheter finnas att förelägga vite.

15.5 Besvärsrätt

På myndighetsnivå kommer alltså att fattas bindande beslut i sårbarhetsfrågor. En möjlighet att föra talan mot sådana beslut måste från rättssäkerhetssynpunkt finnas. De ärenden i vilka sårbarhetsfrågor skall behandlas kommer i många fall att innebära att ett antal olika samhällsintressen måste vägas mot varandra, något som kan vålla en del bekymmer för en fackmyndighet. Med hänsyn härtill bör talan mot besluten föras hos regeringen hos vilken mer övergripande lämplighetsbedömningar kan göras utöver den rent rättsliga prövningen.

Har myndigheten fattat ett beslut som går någon emot har då, enligt vanliga regler, den som beslutet rör rätt att föra talan mot detta. Frågan är om någon även skall ges talerätt vad gäller positiva beslut. Enligt datalagen har JK givits sådan rätt. Detta innebär att JK, som allmänt ombud, kan besvära sig i de fall, då han anser det påkallat för att tillvarata allmänna intressen.

Även när det gäller sårbarhetsfrågor kan det finnas skäl att på motsvarande sätt låta någon, förslagsvis JK, bevaka allmänna intressen.

16 Tillsyn, rådgivning och information

16.1 Tillsynsförfarande

För att kontrollera sårbarhetslagens och meddelade föreskrifters efterlevnad är det som nämnts viktigt att en aktiv tillsynsverksamhet bedrivs. Denna skall omfatta det tillståndspliktiga området. Genom tillsynsverksamheten kan utvecklingen på datorområdet även följas framförallt då vad gäller helt eller delvis nya tilllämpningsområden och följderna av dessa. Tillsynsverksamheten kan även bidra till att sårbarhetsrisker som inte förelegat vid tillståndsförfarandet uppdagas. Som nämnts bör det därför även finnas rätt att, med hänsyn till vad som kommer fram vid en inspektion, ändra givna föreskrifter eller meddela nya. Ytterst bör även ett tillståndsbeslut kunna upphävas. En aktiv tillsynsverksamhet bör alltså drivas. Den får dock inte medföra större kostnader och olägenheter för användarna än nödvändigt.

För att kunna fullgöra tillsynen måste myndigheten ha tillträdesrätt till lokaler där datordriften äger rum. Vidare måste myndigheten ha rätt att ta del av all slags dokumentation rörande system som är underkastade sårbarhetsprövning, och även rätt att föranstalta om körningar av datorer.

Vidare måste myndigheten ha rätt att begära uppgifter och upplysningar av betydelse för tillsynsverksamheten.

Om användaren vägrar tillträde till lokaler eller vägrar att lämna begärda upplysningar bör myndigheten som påtryckningsmedel kunna förelägga vite.

16.2 Rådgivning och information

Hela den offentliga sektorn med undantag av försvarsmakten samt när det gäller den privata sektorn befolkningsregister och register över nyckelpersoner skall alltså enligt SÅRKs förslag underkastas ett tillståndsförfarande. Vidare skall vissa delar av den privata sektorn omfattas av ett anmälningsförfarande.

Som SÅRKs förslag utformats, med hänsyn till övergångsbestämmelserna kommer alla befintliga tillämpningar att falla utanför det tillstånds- och anmälningspliktiga området under en övergångstid på fem år. Vi-

dare kommer stora delar av den privata sektorn att helt falla utanför i vart fall det tillståndspliktiga området. Som tidigare framhållits innebär detta inte att alla dessa delar är ointressanta från sårbarhetssynpunkt. SÅRK har tvärtom utgått från att även här finns behov av olika åtgärder som kan minska sårbarheten. Emellertid har SÅRK ansett att dessa åtgärder kan komma att vidtas även på frivillighetens väg. En förutsättning härför är dock att sårbarhetsmyndigheten bedriver en aktiv rådgivnings- och informationsverksamhet. Ett av huvudskälen till anmälningsförfarandet är för övrigt att det material som kommer in till myndigheten skall kunna användas som underlag för rådgivningsverksamheten. Materialet bör då även kunna användas för att välja ut de områden inom vilka rådgivningsverksamheten är särskilt angelägen.

Rådgivning och information bör åligga sårbarhetsmyndigheten såväl vad gäller tillståndspliktiga som anmälningspliktiga datoranvändare. Även övriga datoranvändare bör kunna vända sig till myndigheten för råd och anvisningar. Genom att myndigheten får en omfattande sakkunskap inom säkerhets- och sårbarhetsområdet bör den kunna vara till stort värde för de användare som behöver expertråd i dessa frågor. Bl a kan myndigheten i det dagliga arbetet samla information och erfarenheter från olika användare och detta kunnande kan sedan komma andra användare med likartade problem till godo. En annan viktig uppgift för myndigheten bör vara att hålla diskussionen och den allmänna debatten vid liv vad gäller sårbarhetsproblem. Mycket är, som tidigare påpekats, vunnet redan genom att användarna blir mer medvetna om dessa problem.

Rådgivningen och informationen kan då gälla val av systemstruktur, metoder för säkerhetsarbete inklusive katastrofplanering, utbildningsbehov osv. I stort sett bör området för rådgivningsverksamheten överensstämma med det som skall prövas vid tillståndsgivningen, något som behandlats ovan. Rådgivnings- och informationsverksamheten kan ske genom uppsökande verksamhet, genom tryckta anvisningar och normer eller i andra lämpliga former.

Olika användare skall på ett tidigt stadium kunna vända sig till tillståndsmyndigheten med frågor som gäller från sårbarhetssynpunkt lämpliga lösningar. Detta bör gälla oavsett om det rör tillståndspliktiga eller andra användningsområden. Det är av största vikt att sårbarhetsaspekterna kommer fram och diskuteras på ett så tidigt stadium som möjligt vid utvecklingen av olika system.

När det gäller tillståndspliktiga system är detta naturligtvis särskilt viktigt genom att systemen härigenom redan från början kan anpassas till de krav som tillståndsmyndigheten ställer. Grundläggande krav bör naturligtvis kunna läsas ut av de författningar som utfärdas i syfte att minska sårbarheten samt ur de tillämpningsföreskrifter och anvisningar som sårbarhetsmyndigheten förutsätts utarbeta. Den rådgivande funktionen bör dock finnas som ett viktigt komplement till dessa källor.

I instruktionen för den myndighet som skall ansvara för sårbarhetsfrågor kan intas bestämmelser om myndighetens rådgivande och informerande funktioner.

De tillståndspliktiga användare som för sin planering och för sina kostnadskalkyler m m på förhand vill veta vilka krav som kan komma att ställas på deras system bör av sårbarhetsmyndigheten redan på projekteringsstadiet kunna begära bindande förhandsbesked.

17 Lämplig myndighet för de föreslagna åtgärderna

I lägesrapporten har SÅRK uttalat att någon redan befintlig funktion i samhället bör anförtros uppgifter av rådgivningskaraktär m m vad gäller sårbarhetsfrågor.

I kapitel 7 har redogjorts bl a för olika myndigheter som har mer eller mindre övergripande funktioner inom ADB-området. Därutöver finns naturligtvis en mängd myndigheter som i sina allmänna göromål kommer i kontakt med ADB-användning på ett eller annat sätt och där även sårbarhetsfrågor kan komma in i bilden. När det gäller t ex kriminella handlingar är detta primärt en uppgift för polis, åklagare och domstolar även om brottsligheten rör ADB. Kriminella handlingar inom ADB-området kan eventuellt vara ett område som även brottsförebyggande rådet kan komma att ägna intresse.

Ansvaret för olika ADB-frågor ligger således spritt på ett flertal händer liksom ansvaret för frågor som mer eller mindre rör samhällets sårbarhet i vid bemärkelse. Av detta följer även att sakkunskap och expertis inom olika delområden finns på spridda håll.

Som nämnts har SÅRK utgått ifrån att någon ny myndighet med uppgift att handha sårbarhetsfrågor inte skall inrättas utan att någon redan befintlig funktion i samhället skall anförtros dessa uppgifter. Flertalet remissinstanser delar denna uppfattning, dock menar några att ansvaret bör kunna läggas på flera olika organ. Av de remissinstanser som utpekat lämplig myndighet har flertalet angett datainspektionen.

Med tanke på de uppgifter som skall åligga tillståndsmyndigheten och att myndigheter inom försvarsmakten undantagits från det reglerade området bör enligt SÅRKs mening i första hand en civil myndighet komma ifråga.

SÅRK anser att de myndigheter som i första hand kan komma ifråga när det gäller huvudansvaret för sårbarhetsfrågor är DI, statskontoret och ÖEF.

Dessa tre myndigheter framstår som centrala vid en diskussion om lämplig myndighet även om det finns flera andra myndigheter med viktiga funktioner som även rör sårbarhetsfrågor t ex SIND och televerket.

När det gäller statskontoret har denna myndighet viktiga uppgifter beträffande rationaliseringsarbete inom statsförvaltningen. Detta har medfört att statskontoret ofta medverkar i samband med utvecklande

och införande av ADB-system. Statskontoret har även viktiga uppgifter när det gäller upphandling av datorer på den statliga sidan. Statskontoret bedriver dessutom ett omfattande datasäkerhetsarbete och har även publicerat ett antal rapporter inom detta område vilket naturligtvis väger tungt. Det finns emellertid skäl som talar emot att statskontoret blir central myndighet vad gäller sårbarhetsfrågorna. Ett skäl är att statskontorets verksamhet är begränsad till den statliga sidan. Ett annat är att statskontoret i första hand är ett rationaliseringsorgan. I samband med rationaliseringsverksamheten deltar statskontoret ofta i systemutvecklingsarbete och som nämnts sköter statskontoret en stor del av upphandlingen när det gäller datorer på den statliga sidan. I det nyligen framlagda betänkandet Rationalisering och ADB i statsförvaltningen föreslås att statskontoret skall behålla en stor del av dessa uppgifter även i framtiden. Dessa uppgifter låter sig inte särskilt väl förena med en sårbarhetsgranskning utan här skulle snarast en rollkonflikt uppstå. Slutligen bör även nämnas att statskontoret inte har några uppgifter när det gäller beredskapsfrågor.

ÖEF har viktiga funktioner vad gäller undanförsel och förstöring beträffande såväl datorer som ADB-lagrad information. Vidare har ÖEF det övergripande ansvaret för att landets försörjning med förnödenheter och tjänster fungerar vid krig, krigsfara och vid fredskriser. Detta gäller även ADB-sektorn. Bl a planlägger ÖEF beredskapen när det gäller datorföretagens underhålls- och servicefunktioner samt verksamheten hos viktigare dataservicebyråer. ÖEF förbereder även krigsproduktionen av förbrukningsmaterial för ADB. Genom sitt ansvarsområde har ÖEF en omfattande kännedom om företag, organisationer m m som till viss del även skulle kunna användas i samband med den rådgivande verksamhet som diskuterats i ett tidigare avsnitt. ÖEF har dessutom uttryckligen getts vissa uppgifter vad gäller myndigheters planläggning av informationsbehandling i krig. Vidare har ÖEF ansvaret för att näringslivet har tillgång till datorkraft som är nödvändig även vid beredskapstillstånd och krig. Detta följer av ÖEFs allmänna uppgifter.

DI har en särställning genom att den huvudsakliga uppgiften består i att bevaka frågor som sammanhänger med användningen av ADB. DI är alltså den enda renodlade datamyndigheten. Genom att DI idag endast har granskande uppgifter finns det heller ingen risk för kompetenskonflikter inom myndigheten. DIs område är visserligen begränsat till integritetsfrågor och personregister förda med ADB-teknik men trots denna begränsning har inspektionen en ganska god överblick över ADB-användningen inom landet. Detta beror bl a på att ett stort antal ADB-verksamheter ofta har åtminstone något inslag av personregistrering som omfattas av datalagen.

Det som främst talar mot DI är att denna myndighet i dag inte har några beredskapsplanerande uppgifter och således inte någon erfarenhet av sådan planering.

Prövning av sårbarhetsfrågor vad gäller personregister med känsligt innehåll och befolkningsregister är en uppgift som det faller sig naturligt att DI handhar. Inspektionen har för övrigt redan ett stort underlag när

det gäller dessa register, ett underlag som kan användas vid rådgivningsverksamheten. En stor del av datoranvändningen inom den offentliga sektorn rör för övrigt personregister och samma sak gäller viktiga delar av den privata sektorn t ex bank- och försäkringssidan. DI kan då, på delvis samma underlag och i ett sammanhang göra integritets- och sårbarhetsprövningen. Bara det förhållandet att användarna slipper gå till flera myndigheter för att få personregister prövade måste här väga tungt. För övrigt kan många av de åtgärder som vidtas för att minska riskerna för intrång i den personliga integriteten även bidra till att minska sårbarheten i olika avseenden. Bland inspektionens uppgifter ingår även ADB-säkerhetsarbete.

Om man med detta resonemang konstaterar att DI bör bevaka sårbarhetsfrågorna inom en förhållandevis stor sektor blir nästa fråga om även övriga delar bör läggas på samma ställe. Vad som då avses är administrativa ADB-system med annan information än personinformation där bedömningarna för övrigt bör bli rätt likartade samt områden som trafikstyrning, processtyrning etc. Som framgått har ÖEF många anknytningspunkter till olika sårbarhetsfrågor bl a inom dessa områden och ett alternativ är att lägga huvudansvaret på ÖEF.

Vid en samlad bedömning finner SÅRK dock övervägande skäl tala för att DI handhar sårbarhetsfrågorna även inom nu diskuterat område. Ett av de tyngre skälen härför är att sårbarhetsfrågorna, enligt SÅRKs mening, i så stor utsträckning som möjligt bör samlas hos en och samma myndighet. En sådan lösning ger bättre förutsättningar för enhetliga bedömningar och ger även andra fördelar för användarna.

Slutsatsen blir alltså att DI är den myndighet som skall åläggas huvudansvaret för sårbarhetsfrågor inom samtliga områden.

Huvudansvaret för sårbarhetsfrågor läggs alltså hos DI. Emellertid berörs även en mängd andra myndigheter av sårbarhetsfrågor varav några mer centralt. Ett stort behov av samråd mellan de olika myndigheterna föreligger därför. Ibland måste sådant samråd vara obligatoriskt bl a därför att ansvarsgränserna i vissa fall är flytande. Framförallt kommer samarbete mellan ÖEF och DI att krävas i stor utsträckning eftersom de båda myndigheternas arbetsuppgifter ofrånkomligen kommer att vara sammanvävda.

Visserligen har DI en styrelse med bred sammansättning. Det finns emellertid enligt SÅRKs mening behov av ett rådgivande organ i sårbarhetsfrågor, knutet till DI.

Ett sådant råd bör bestå av experter som kan belysa olika sårbarhetsaspekter och bidra till lösningar på olika sårbarhetsproblem. Representerade i ett sådant råd bör vara bl a försvarsdepartementet, ÖEF, ÖB, RPS, televerket, statskontoret och DAFA. Vidare bör kommunerna och näringslivet vara representerade. Det rådgivande organet förutsätts i första hand ägna sig åt principiella övergripande frågor av intresse när det gäller olika sårbarbarhetsaspekter.

DI har i dag en organisation med en administrativ enhet samt en tillstånds- och en tillsynsenhet. Frågan är om en särskild enhet för sårbarhetsfrågor bör inrättas eller om de redan existerande tillstånds-

och tillsynsenheterna skall förstärkas och således då även ta hand om sårbarhetsfrågorna. Även andra alternativ är tänkbara. SÅRK finner ingen anledning att nu förorda någon bestämd lösning i detta avseende. Eventuellt kan man tänka sig att DI blir föremål för en organisationsöversyn. Vad SÅRK dock vill framhålla är att sårbarhetsfrågorna måste ges en framskjuten plats i verksamheten.

18 Överväganden kring andra åtgärder

18.1 Utlandsberoendet och den svenska datorindustrins konkurrenskraft

När det gäller utlandsberoendet är detta som nämnts en fråga som till stor del rör den svenska industrins konkurrenskraft inom datorområdet. Bevakningen av dessa frågor åligger redan SIND och i viss mån de utredningar som nämnts. Någon anledning att ändra på ansvarsområdet härvidlag finns inte. Däremot kan det finnas skäl att ägna dessa frågor ännu större intresse mot bakgrund av deras stora betydelse från sårbarhetssynpunkt.

18.2 Reservdelsförsörjning m m

När det gäller planeringen av hur ADB-verksamheten skall kunna hållas igång under krig, krigsfara och vid s k fredskriser har ÖEF som nämnts ett övergripande ansvar idag, något som följer av ÖEFs allmänna ansvar för näringslivet i krissituationer. I detta uppdrag ligger även frågor som rör reservdelsförsörjning, tillgång till förbrukningsmaterial etc.

Det torde inte vara realistiskt att förutsätta någon större minskning av importberoendet av datorer med kringutrustning, reservdelar och komponenter även vid större satsningar på svensk datorindustri. Förutsättningarna att kompensera importberoendet genom statlig beredskapslagring av reservdelar och komponenter måste också anses mycket tveksamma p g a den höga förnyelsetakten, det stora antalet erforderliga reservdelar och komponenter samt de kostnader som en beredskapslagring av kuranta artiklar skulle innebära.

För att minska riskerna med importberoendet bör i avtal om köp av datorer m m om möjligt införas bestämmelser om lagerhållning i landet av reservdelar m m och garantier om service även i situationer då utrikeshandeln är störd. Särskilt bör detta beaktas vid större offentliga upphandlingar.

I importberoendet i vid bemärkelse ingår också behovet av tekniskt kunnande. Detta problem kan endast lösas genom långsiktiga åtgärder på utbildningens område. Mot denna bakgrund är det nödvändigt att sådana åtgärder vidtas snarast.

Till de mer utpräglade beredskapsåtgärderna bör höra föreberedelser för omfördelning av datorkraft i ett beredskapsläge eller krigsläge då sabotagehandlingar kan befaras. Härigenom kan säkerställas att samhällsnödvändiga datasystem kan hållas i drift utan alltför långvariga avbrott. För att möjliggöra en sådan omfördelning (back-up för högt prioriterade system) måste tillgången på olika slag av datorer m m i landet och dessas lokalisering kontinuerligt följas. Denna uppgift och anvisande av back-up-anläggning bör också fortsättningsvis åvila ÖEF. Om nödvändigt behov av reservdelar eller komponenter inte kan tillgodoses på annat sätt bör ÖEF också i ett krigsläge kunna ge anvisning på datorer som kan slaktas.

För undanförsel och förstöring gäller lag och kungörelse (1961:655 — 656) härom samt av ÖEF meddelade tillämpningsanvisningar (Anvisningar för undanförsel, Anvisningar för undanförsel av arkivalier, Anvisningar för förstöring). Närmare beskrivning av olika metoder att förstöra datalagrad information bör dock meddelas. Som nämnts bör DI förse ÖEF med underlag för bedömningar i dessa frågor.

18.3 Ansvaret för datakommunikationer

Televerket har som nämnts ett viktigt ansvar när det gäller datakommunikationer och verket har även ansvar för sårbarhetsfrågor. Televerket bör naturligtvis även fortsättningsvis ha detta ansvar. Det är dock viktigt att samråd sker med andra myndigheter som har eller kommer att få ansvar för sårbarhetsfrågor främst då DI.

18.4 Personalsamordning mellan den militära och civila sidan

När det gäller personalsamordningen mellan det militära försvaret och den civila sidan får detta lösas genom samverkan mellan civila arbetsgivare och försvarets myndigheter inom ramen för krigsuppskovsförfarandet.

18.5 Standardisering och utbildning

Det finns även en del andra sårbarhetsproblem som inte kan lösas inom ramen för ett tillståndsförfarande. Hit hör t ex bristen på standardisering och utbildning. Dessa frågor bör naturligtvis bevakas av berörda myndigheter. DI bör då beakta verkningarna från sårbarhetssynpunkt och ge förslag till statsmakterna om åtgärder som kan förbättra situationen.

18.6 Skyddet för företag

I samband med datalagens tillkomst diskuterades frågan om reglerna för dataregistrering borde utformas så att de gav skydd inte bara för enskil-

das personliga integritet utan också för andra intressen t ex rikets säkerhet och enskilda företags integritet. Reglerna inskränktes dock som bekant till att tillgodose skyddet för den personliga integriteten. Däremot omfattar vissa utländska datalagar som tidigare nämnts även juridiska personer.

SÅRK har pekat på att allt större mängder företagsdata lagras i offentliga datasystem och att sekretesskyddet kan vara bräckligt bl a genom att det ibland försvinner när uppgifterna sprids till andra myndigheter. I avsnitt 5.1.2 redogörs även för en skrivelse från Sveriges Industriförbund i vilken dessa problem tas upp. Liknande synpunkter har framkommit från Industriförbundet och SAF i samband med remissbehandlingen av SÅRKs lägesrapport.

Från sårbarhetssynpunkt har frågan betydelse bl a för det ekonomiska försvaret. Som SÅRK påpekat ökas även möjligheterna att framgångsrikt bedriva industrispionage, en typ av spioneri som för övrigt blivit allt vanligare på senare år. Antagandet att denna typ av spioneri fått en ökad omfattning var ett av skälen till att spionbrottsutredningen tillsattes. Utredningen har nu avgivit betänkandet Översyn av spioneribrottet m m (Ds Ju 1979:6). Utredningen har också funnit att det finns mycket som talar för att den främmande underrättelseverksamheten under de senaste decennierna alltmer inriktats på politiska, ekonomiska och industriella förhållanden. I denna del föreslår utredningen att spioneriparagrafen skall förtydligas så att det klart framgår att bestämmelsen kan tillämpas på politiskt och ekonomiskt spionage. Utredningen framhåller emellertid att det av olika skäl endast är i speciella situationer som industrispionage och politiskt spionage kan komma att falla under spionerilagstiftningen. Två reservanter föreslår dock ändringar som i större omfattning skulle täcka gärningar av nu diskuterat slag.

Det kan även nämnas att vissa förfaranden är straffbara enligt andra bestämmelser bl a enligt lagen med vissa bestämmelser mot illojal konkurrens.

Nyligen har en särskild utredare (Ju 1979:09) tillkallats med uppgift att utreda skyddet för företagshemligheter m m. I direktiven till utredaren sägs bl a att det är en påtaglig brist att de f n saknas särskilda bestämmelser som riktar sig mot industrispionage och att utredaren bör ge förslag till effektivare regler på detta område.

När det gäller sekretesslagstiftningen har den nyligen undergått en genomgripande översyn som nu resulterat i en proposition (1979/80:2) till riksdagen med förslag till sekretesslag m m. Såvitt SÅRK kunnat finna har inte några avgörande ändringar i sak föreslagits vad gäller sekretesskydd för företag.

Vissa av de förslag SÅRK har lagt fram bör kunna bidra till att komma till rätta med nu diskuterade sårbarhetsproblem. Som exempel kan nämnas granskningen av registerinnehåll, prövning av i vad mån samkörning och integrering bör tillåtas, föreskrifter om kryptering och behörighetssystem m m.

Frågan är emellertid om ytterligare åtgärder är nödvändiga och i så fall vilka. Bör t ex strafflagstiftningen och sekretesslagstiftningen skär-

pas. Finns det skäl att införa ytterligare begränsningar — utöver den som skett genom Delegationens (B 1977:09) för företagens uppgiftslämnande m m (DEFU) verksamhet — i myndigheters rätt och möjligheter att samla information. SÅRK är inte beredd att svara på dessa frågor i nuvarande läge. Det finns dock skäl att tillståndsmyndigheten följer utvecklingen inom detta område och försöker ge eventuella förslag till lämpliga åtgärder eller i vart fall ge underlag som kan ligga till grund för sådana åtgärder.

18.7 Vissa problem som sammanhänger med användning av annan teknik än datatekniken

SÅRKs utredningsuppdrag enligt direktiven tar sikte på den sårbarhet som datoriseringen för med sig. Det kan emellertid finnas skäl att peka på att nya tekniska hjälpmedel — som inte är hänförliga till ADB-området — utvecklas, t ex mikrofilms- och mikroficheteknik, som delvis ger samma möjligheter som ADB. Det kan gälla t ex lagring och bearbetning samt snabb återvinning av stora informationsmängder.

Vad gäller befolkningsregister och register med känslig information som förs med hjälp av sådan teknik kan i stort sett samma argument föras fram vad gäller sårbarhetsriskerna som om registren förs med hjälp av ADB.

DALK har i sitt delbetänkande, Personregister-Datorer-Integritet (SOU 1978:54), skisserat en framtida personregisterlag som bland annat skulle innebära en reglering av all registrering och därmed jämförlig användning av personuppgifter som kan innebära farhågor för otillbörligt intrång i den personliga integriteten. Detta oavsett vilken teknik som används vid registreringen. Som ett skäl härför anges de möjligheter som andra tekniska hjälpmedel än ADB medför.

Måhända kommer DALKs fortsatta arbete med en personregisterlag att kunna ge en närmare beskrivning av vilka tekniker som kan mäta sig med ADB-tekniken vad gäller lagrings- och bearbetningsmöjligheter m m. Frågan om en reglering utifrån sårbarhetsaspekten av befolkningsregister och andra från sårbarhetssynpunkt känsliga register som förs med annan teknik bör därför vila i avvaktan på DALKs utredningsresultat i nämnda hänseende.

19 Sammanfattning av SÅRKs förslag

19.1 Tillstånd inom den offentliga sektorn

SÅRKs förslag innebär att datoranvändning inom hela den offentliga sektorn med undantag av försvarsmakten skall underkastas en sårbarhetsprövning. Prövningen skall ske i form av tillståndsförfarande. Användning som uppenbarligen inte kommer att medföra risker från sårbarhetssynpunkt skall undantas från prövning genom en generell dispensregel. Vad som avses bli undantaget får bestämmas närmare av regeringen eller av myndighet som regeringen bestämmer enligt vissa allmänna riktlinjer.

Tillståndsplikten gäller inte datoranvändning som beslutats av regering och riksdag. Före sådant beslut skall dock ansvarig myndighet höras.

19.2 Tillstånd inom den privata sektorn

När det gäller den privata sektorn föreslår SÅRK ett tillståndsförfarande vad avser ADB-baserade befolkningsregister och register över persongrupper som kan vara av intresse för utländsk underrättelsetjänst.

19.3 Tillståndsmyndighet, tillståndsprövning och föreskriftsmöjlighet

SÅRK föreslår att DI skall fungera som tillståndsmyndighet.

En tillståndsprövning skall enligt SÅRK omfatta registerinnehåll, systemstruktur, ADB-säkerhet, personalberoende, maskinella och och manuella reservrutiner, katastrofplanering, dokumentation, integration och beroende av andra databehandlingssystem, geografisk lokalisering och utlandsbearbetningar. När det gäller dessa punkter skall även erforderliga föreskrifter för att minska sårbarheten ges. I undantagsfall kan tillstånd nekas.

När register inte längre skall föras skall detta anmälas till DI som skall föreskriva hur det skall förfaras med registren.

Föreskrifter när det gäller datoranvändning som beslutats av stats-

makterna skall ges av tillståndsmyndigheten om inte statsmakterna har gett föreskrifter i samma hänseende.

19.4 Anmälan och myndighet till vilken denna skall ges in

SÅRK föreslår att en anmälningsplikt skall införas för datoranvändande företag och organisationer som anses som särskilt viktiga för landets försörjning. För att få fram dessa företag föreslår SÅRK att ÖEFs förteckning över s k K-företag skall användas. I denna förteckning finns de företag som ÖEF finner vara av särskild betydelse när det gäller att tillgodose landets behov av förnödenheter och tjänster under krig. Det bör ankomma på regeringen att närmare ange de företag inom denna krets som skall underkastas anmälningsplikt.

Anmälan bör omfatta uppgifter om maskinell utrustning, dess lokalisering och användningsområde, systemstruktur, ADB-säkerhet, katastrofberedskap och typ av registerinnehåll. Anmälan skall alltid innehålla uppgift om de utlandsbearbetningar som förekommer.

Som det huvudsakliga skälet till en sådan anmälningsplikt har SÅRK angivit att den underlättar en aktiv rådgivnings- och upplysningsverksamhet. Det material som på detta sätt kommer in till myndigheten kan användas som underlag för rådgivning inom de viktigaste delarna av privatsektorn. Materialet behövs även, enligt SÅRKs mening, som underlag för den fortsatta diskussionen av frågor som rör sårbarhetssituationen i landet och hur denna skall bemästras.

SÅRK föreslår att DI skall ha huvudansvaret för rådgivningsfunktionen inom detta område. Anmälningarna skall således ges in till denna myndighet. Samråd och samarbete förutsätts dock ske mellan DI och ÖEF.

19.5 Rådgivning och information

SÅRKs förslag innebär att endast vissa delar av samhällets datoranvändning skall omfattas av en tillståndsprövning. En utgångspunkt för SÅRK har emellertid varit att en aktiv rådgivnings- och informationsverksamhet skall förekomma inom såväl det tillståndspliktiga området som inom övriga områden. SÅRK anser att denna del av verksamheten måste ägnas stor uppmärksamhet.

När det gäller tillståndspliktiga användare skall dessa även kunna begära bindande förhandsbesked av DI.

19.6 Tillsyn och tillsynsmyndighet

DI skall enligt förslaget även utöva tillsyn inom det tillståndspliktiga området. I samband med tillsynen kan ändrade föreskrifter ges och i undantagsfall kan meddelat tillstånd återkallas.

19.7 Dataservicebyråverksamhet

Även dataservicebyråverksamhet omfattas av förslaget. Prövningen och föreskrifterna får dock begränsas till de punkter för vilka ansvaret, helt eller delvis, naturligt ligger på servicebyrån. Främst gäller detta ADB-säkerhet, personalberoende, dokumentation, reservrutiner, katastrofplaner och utlandsbearbetningar. Vad avser statligt och kommunalt ägda servicebyråer gäller tillståndsplikten i samma omfattning oavsett om verksamheten drivs i myndighets- eller bolagsform.

19.8 Övergångsbestämmelser

SÅRKs förslag gäller i första hand nya tillämpningar och sådana tillämpningar som undergår väsentliga förändringar. För datoranvändning som påbörjats före ikraftträdandet gäller lagen efter en femårig övergångstid om inte väsentliga ändringar gjorts dessförinnan, för vilket fall lagen gäller från tidpunkten för förändringen. Anmälan behöver, för användning som påbörjats före lagens ikraftträdande endast ske då väsentliga förändringar görs. Även för äldre tillämpningar förutsätts rådgivning kunna ske.

19.9 Besvär

Talan mot datainspektionens beslut kan enligt förslaget föras hos regeringen. JK kan föra talan för att tillvarata allmänna intressen.

19.10 Rådgivande organ

SÅRK har även föreslagit att en rådgivande funktion vad gäller sårbarhetsfrågor skall inrättas med representanter från bl a berörda departement, myndigheter och näringslivsorganisationer. Det rådgivande organet, som skall knytas till DI förutsätts i första hand ägna sig åt principiella övergripande frågor av intresse när det gäller olika sårbarhetsaspekter.

20 Resurs- och kostnadsberäkningar

20.1 Allmänt

SÅRKs förslag innebär tillståndsprövning inom den offentliga sektorn och inom den privata sektorn vad avses befolkningsregister och register över nyckelpersoner. Ett anmälningsförfarande skall gälla för vissa av de s k K-företagens datoranvändning. Bestämmelserna tar i första hand sikte på nya tillämpningar och tillämpningar som undergår väsentliga förändringar. Anmälningarna skall användas som underlag för en aktiv rådgivningsverksamhet. Det tillståndspliktiga området skall stå under tillsyn. DI skall vara tillstånds- och tillsynsmyndighet.

En viktig del av DIs verksamhet kommer att bestå i att avge remissyttranden till regeringen vad gäller den statliga datoranvändningen. Andra viktiga verksamheter kommer att vara utvecklingsarbete, utfärdande av anvisningar, medverkan till en närmare utformning av dispensregeln samt rådgivnings- och informationsverksamhet.

20.2 Tillståndsärenden och ärenden som rör datoranvändning som beslutats av statsmakterna

Det dominerande antalet tillståndsärenden kommer att gälla datoranvändning inom den offentliga sektorn. SÅRK har tagit antalet datalagsärenden som utgångspunkt vid ett försök att bedöma den mängd ärenden förslaget kommer att medföra. Till DI inkom under budgetåret 1978/79 ca 3 500 ärenden varav ca 3 000 rör datalagen. De ärenden som gällde statliga register uppgick till ca 600 och de som gällde kommunala register uppgick till ca 650. Aktuella siffror (nov 1979) rörande ärendemängd tyder på att totalsiffrorna för innevarande budgetår kommer att bli högre.

Som SÅRK tidigare påpekat sker datoranvändning inom den offentliga sektorn i regel inom administrativa och liknande områden. Detta medför att datasystemen i stor omfattning innehåller personregister. Det finns emellertid användningsområden på den offentliga sidan som saknar inslag av personregistrering. Denna del är dock förmodligen ganska liten.

Om man utgår från de ca 1 200 ärenden som gällde offentliga register under föregående budgetår bör åtminstone 25 % hamna inom det om-

råde som blir föremål för dispens enligt SÅRL. Å andra sidan tillkommer ett antal ärenden som rör tillämpningar som saknar inslag av personregistrering. Vidare tillkommer ett antal tillstånds- och anmälningsärenden från den privata sektorn. Dessutom får man räkna med viss osäkerhet när man använder siffror som gäller datalagen eftersom det är delvis andra frågor som skall prövas vid en sårbarhetsbedömning.

Med utgångspunkt från de siffror som angivits kan man dock anta att antalet ärenden om tillstånd, och ärenden som föranleds av datoranvändning som beslutas av statsmakterna, kan beräknas till drygt 1 000 årligen.

Tidsåtgången för att granska olika tillämpningar kommer att variera ganska kraftigt. För större statliga och kommunala system kan det röra sig om stor tidsåtgång där dessutom handläggningen utsträcks under lång tid. En del ärenden kan å andra sidan antagligen klaras av på några timmar. Det finns dock skäl att anta att sårbarhetsprövningen i regel, med tanke på alla de faktorer som skall beaktas, kommer att vara mera tidskrävande än prövningen enligt datalagen.

Med de övergångsbestämmelser SÅRK förelagit kommer det inte att finnas någon ingående balans av tillståndsärenden. Däremot kommer en tillfällig ökning av ärenden att ske vid den femåriga övergångstidens slut. Hur stort detta antal kommer att bli är svårt att förutse. Denna extra belastning torde dock till stor del kunna mötas genom att en del av de personella resurser som krävs i inledningsskedet t ex för utvecklingsarbete, för att utge anvisningar etc efterhand kan överflyttas till andra arbetsuppgifter. Vid femårsfristens slut bör även arbetet flyta bättre genom den rutin och erfarenhet handläggarna har skaffat sig.

20.3 Anmälningsärenden och rådgivning

SÅRK har föreslagit att vissa av de s k K-företagen skall omfattas av en anmälningsplikt. Antalet företag som kan antas beröras av anmälningsförfarandet uppgår till ca 2 000. Eftersom det endast är nya tillämpningar eller tillämpningar som underkastas väsentliga förändringar kan antalet anmälningsärenden uppskattas till ca 300 per år.

Som nämnts skall anmälningsärenden underkastas en aktiv rådgivningsverksamhet. Det underlag som kommer in i samband med anmälan skall utgöra underlag för denna verksamhet. Genomgången av materialet och övrigt arbete som måste läggas ner på rådgivningsverksamheten kommer många gånger att kräva lika stora arbetsinsatser som en tillståndsprövning. Rådgivningsverksamheten kommer överhuvudtaget — och alltså inte endast inom det anmälningspliktiga området — att kräva relativt stora arbetsinsatser.

20.4 Tillsynsverksamheten

Tillsynsverksamhet skall utövas inom det tillståndspliktiga området. Det kan nämnas att tillsynsärenden enligt datalagen uppgick till ca 100 under föregående budgetår.

Det kan antas att tillsynsverksamheten inte kommer att bli lika arbetskrävande som tillstånds- och rådgivningsverksamheten i vart fall inte till en början. De olika verksamheterna bör dock ske i nära samband. Tillsynsverksamheten kommer givetvis att medföra en del resekostnader.

20.5 Metodutveckling, forskning, arbete med att utfärda anvisningar och föreskrifter

Ett omfattande arbete kommer att krävas, framförallt i inledningsskedet av lagens tillämpning, vad gäller t ex arbete med metodutveckling för sårbarhets- och säkerhetsanalyser och annat forskningsarbete. Det måste även till stor del ankomma på DI att få fram närmare beskrivningar av vad som skall undantas från lagens tillämpningsområde enligt den generella dispensregeln. Vidare skall anvisningar och tillämpningsföreskrifter som gäller övriga delar av lagens utfärdas. Olika arbetsrutiner och blanketter måste utarbetas osv.

20.6 Personalbehov

För att klara den arbetsmängd och de arbetsuppgifter som beskrivits krävs minst 12 handläggare. Vidare krävs 4 biträden för skrivuppgifter, expeditionsarbete, registreringsarbete m m. För handläggande personal kommer det att röra sig om uppgifter av delvis mycket kvalificerat slag. Tjänsterna bör därför ligga förhållandevis högt på den statliga löneskalan. Det kan för övrigt ifrågasättas om man inte måste gå utanför denna skala för att överhuvudtaget kunna anställa viss kvalificerad teknisk personal, som kommer att erfordras. Några tjänster bör därför kunna tillsättas genom kontraktsanställning.

Behov kommer även att finnas av att köpa tjänster utanför organisationen. Medel måste därför anvisas som gör det möjligt att anlita konsulter.

20.7 Kostnader för myndighet m m

SÅRK har beräknat kostnaderna under ett budgetår enligt följande

Lönekostnader	2 145 000
Konsultarvoden	100 000
Ersättning till styrelse och rådgivande organ	150 000
Resor	80 000
Diverse utgifter för bl a lokaler, expenser	375 000
Information	50 000
	2 900 000

Under första budgetåret kommer vissa kostnader att ligga högre eller utgöra initialkostnader. Bl a kommer kostnaderna för information att ligga högre eftersom berörda grupper måste få vetskap om tillkomsten av en helt ny lag. Vidare kommer konsulter att behöva anlitas i högre grad under inledningsskedet bl a för att medverka i metodarbete m m.

Merkostnaderna under första året kan beräknas enligt följande

Konsultarvoden	200 000
Information	50 000
Platsannonser m m	35 000
Inventarier	100 000
	385 000

De sammanlagda kostnaderna under första budgetåret skulle sålunda uppgå till 3 285 000 kr.

20.8 Övriga kostnader

SÅRKs förslag kommer givetvis att medföra kostnader även för datoranvändarna. Hur stora dessa kostnader kommer att bli är dock praktiskt taget omöjligt att beräkna. Som SÅRK tidigare påpekat bör dock en strävan vara att hålla kostnaderna på en rimlig nivå för användarna. Genom att förslaget i första hand tar sikte på nya tillämpningar kan olika åtgärder planeras in redan från början. Merkostnaderna för åtgärder som minskar sårbarheten kan då många gånger bli försumbar. Även om sådana åtgärder medför extra kostnader måste man mot dessa väga det värde som ligger i den ökade säkerheten. Kostnaden kan då jämföras med en försäkringspremie. Man kan även tänka sig situationer där valet står mellan utifrån olika aspekter — kostnadsmässiga och andra — förhållandevis jämbördiga alternativ där ändå ett av alternativen framstår som bättre när det gäller att hålla sårbarheten på en rimlig nivå.

När det gäller själva ansöknings- och anmälningsförfarandet kommer detta att medföra visst arbete och vissa kostnader för användarna. Som tidigare nämnts gäller dock förslaget till stora delar datoranvändare som ändå måste ge in ansökningar — på grund av datalagens bestämmelser — med delvis samma innehåll som det som behövs för sårbarhetsprövningen.

21 Reservationer och särskilda yttranden

21.1 Reservation av ledamöterna Olof Hertz och P-G Vinge

Som närmare belyses i avsnitt 17 i betänkandet har ÖEF författningsenligt ett övergripande ansvar för att bl a ADB-sektorns försörjning med förnödenheter och tjänster fungerar i kris och krigstider. Till följd av denna instruktionsmässiga uppgift upprättar ÖEF en särskild försörjningsplan för ADB-sektorn som grund för sin beredskapsplanläggning av datorföretagens underhålls- och servicefunktioner samt av krigsproduktion av förbrukningsartiklar för ADB. ÖEF förbereder också verksamheten hos viktigare dataservicebyråer. För att fullgöra sina uppgifter måste ÖEF ha god kunskap om bl a datorbeståndet i landet, användningsområden och grad av datorberoende inom både offentlig förvaltning och näringslivet. ÖEF har därför från landets från försörjningssynpunkt viktiga företag, främst K-företagen, insamlat ett omfattande material om företagens informationsbehandling (begreppet här använt i dess vidaste bemärkelse). Uppgifternas aktualitet kontrolleras kontinuerligt i samband med företagsbesök med biträde av bl a länsstyrelsernas försvarsenheter i syfte att anpassa förändringar i datorutnyttjandet till beredskapsplaneringens krav.

Den samverkan mellan näringlivet och ÖEF som det här gäller har pågått långt innan ADB togs i bruk. Ett utbrett och väl inövat kontaktnät mellan den ansvariga myndigheten och K-företagen finns m a o sedan lång tid tillbaka. Såvitt vi förstår kan det inte vara fråga om att lösa ÖEF från dess nuvarande skyldigheter. Vilket alternativ som än väljs måste ÖEF också framgent samla in alla de uppgifter som behövs för beredskapsplaneringen inom hela datorområdet, alltså även väsentliga uppgifter från näringslivet.

Det är enligt vår mening ofrånkomligt att den samlade och från totalförsvarssynpunkt mycket känsliga information det här är fråga om inte får större spridning än som är absolut nödvändigt. Denna uppfattning speglas för övrigt av föreskrifterna i SFS 1948:390 4 § där det sägs

Uppgifter angående näringsidkares verksamhet, som införskaffats jämlikt 1 § eller eljest erhållits i samband med planläggningen av den ekonomiska försvarsberedskapen, må ej yppas i vidare mån än som erfordras för planläggningen (Lag 1975:693).

I vad avser den föreslagna sårbarhetslagens tillämpning på näringslivet utom beträffande personregister gäller det inte att meddela tvingande föreskrifter utan att genom rådgivning få till stånd en minskad sårbarhet och stärkt oberoende. Detta mål anser vi bäst kunna nås genom att utnyttja den särskilda kompetens som redan finns hos ÖEF i fråga om näringslivets datorutnyttjande. Under alla omständigheter avvisar vi tanken på att till en enda myndighet centralisera sårbarhetsprövningen av samhällets totala informationsbehandling.

Sårbarhetsprövning i vid mening innefattar många fler faktorer än informationsbehandling med hjälp av ADB. En sådan mer omfattande prövning måste genom ÖEFs försorg utföras i samband med beredskapsplanläggningen av K-företagen. Vi förordar därför som det mest naturliga och ändamålsenliga att ÖEF åläggs att utöva den rådgivande funktionen till näringslivet enligt SÅRKs förslag. Genom vårt förslag minskas för övrigt också behovet av personalökningar.

21.2 Särskilt yttrande av ledamoten Jan Freese

Kommittén har funnit att den sårbarhet som orsakats genom den hittills genomförda datoriseringen blivit oacceptabelt hög. Förklaringen härtill är bl a bristen på styrning av den utveckling som lett fram till dagens genomdatoriserade samhälle. Helhetsbedömningar liksom riktlinjer har saknats både på den offentliga och den privata sektorn.

Mot den bakgrunden är det också enligt min mening nödvändigt att åtgärder snarast vidtas för att motverka att den fortsatta datoriseringen i onödan ökar den allmänna sårbarhet som kännetecknar det moderna teknik- och importberoende samhället. Jag vill utveckla min syn på denna fråga på följande sätt.

Utnyttjande av datorer, såväl generella som minidatorer och mikroprocessorer, används inom samhällets alla områden. Sårbarhetsproblemen har i stort sett samma spridning. De åtgärder som bör vidtas bör så långt möjligt vara gemensamma för likartade problem oavsett inom vilket samhällsområde de förekommer.

Både geografisk och funktionell koncentration finns inom båda sektorerna. Verksamhet av betydelse för t ex penningströmmarna är inte uteslutande koncentrerad till en av dem. Känslig eller annan för t ex spioneri eller industrispionage åtråvärd information förekommer på alla samhällsområden. Sabotage eller andra surrogatkrigsåtgärder eller rena krigshandlingar utgör i lika hög grad hot mot databehandlingsverksamhet av betydelse för samhällets sårbarhet, oavsett om denna bedrivs i samhällets regi eller privat. Databehandlingsverksamhet som är externt beroende av annan sådan verksamhet förekommer både på den offentliga och den privata sektorn. Dessutom förekommer ett stort beroende över sektorsgränserna. Det funktionsmässiga beroendet och integreringen begränsar kraftigt antalet verksamheter som är att betrakta som självständiga och således kan fungera isolerade från andra. Risk för oavsiktliga fel förekommer inom båda sektorerna. Strejker kan inträffa

både inom offentlig och privat verksamhet. Katastrofer och olyckshändelser som t ex brand och översvämningar utgör ett hot oavsett om verksamheten bedrivs i offentlig eller privat regi. Personalberoendet är liksom utlandsberoendet och beroendet av reservdelar och service ett lika stort problem inom den offentliga förvaltningen som inom näringslivet. Det bör slutligen uppmärksammas att vad som är offentlig eller privat verksamhet ibland bara beror på en formell bestämning.

Vissa skillnader förekommer dock mellan den offentliga och den privata sektorn. Hos stat och kommun är verksamheten huvudsakligen av administrativ karaktär och denna är i sin tur till övervägande delen koncentrerad till persondata. Inom näringslivet förekommer också sådan verksamhet till betydande grad men dessutom används väsentligt mer än inom den offentliga sektorn processtyrnings-, lagerstyrnings- och distributionssystem. Även beträffande beroendet av internationella datanät och datorkraft i utlandet föreligger en skillnad. Sådant beroende är klart störst inom näringslivet. I händelse av beredskaps- och krigssituationer torde också uppkomma en skillnad. Beroendet av fungerande databehandlingsverksamhet på den privata sektorn torde volymmässigt minska medan det sannolikt ökar på den offentliga sektorn, bl a på grund av administrationen av ransoneringssystem m m samtidigt som den nuvarande utformningen av verksamheten gör att det starkt kan ifrågasättas om administrativ databehandling hos många civila myndigheter kan över huvud taget upprätthållas i krigstid.

Även om det finns vissa skillnader gäller alltså enligt min mening att sårbarhetsfaktorerna i princip omfattar både offentlig och privat verksamhet. Sårbarhetseffekterna kan också nå likartad omfattning på båda sektorerna. Det är egentligen bara fråga om gradskillnader.

Mot denna bakgrund bör reglerna utformas lika för alla samhällsområden. Skillnaderna i åtgärderna inom offentlig eller privat sektor blir då beroende av verksamheten som sådan och inte av en i detta sammanhang kanske helt ovidkommande klassificering i offentlig eller privat verksamhet.

Samtidigt saknas anledning att göra något generellt undantag från regleringen annat än för sådan databehandlingsverksamhet inom försvarsmakten som skall användas i beredskap och krig. Det finns lika litet skäl att undanta övriga delar av försvarsmaktens verksamhet som att undanta databehandlingsverksamhet inom polisen, civilförsvaret, det ekonomiska försvaret osv. Tvärtom är det kanske på dessa och likartade områden viktigare än på andra att man kan dra nytta av den sakkunskap samhället kan tillhandahålla till skydd för databehandlingsverksamhet.

Tekniskt sett är möjligheterna att utnyttja tekniken i olika sammanhang nästan utan begränsningar. Det är därför mycket svårt att avgränsa den verksamhet som är av betydelse för samhällets sårbarhet. Det är en allt vanligare situation att det till följd av ny teknik eller samhällets komplexitet tyvärr bara blir svårare och svårare att med traditionell lagstiftningsteknik skapa normer i syfte att styra utvecklingen. Integritetsproblemet är ett exempel. Ett annat kan hämtas från taxeringsområdet där man numera anser sig behöva tillgripa s k generalklausuler.

Traditionella normgivningsmetoder blir svåra att tillämpa.

Grovt angivet föreligger egentligen, för att förhindra sårbarhetseffekter av betydelse för samhällets sårbarhet inom offentlig eller privat verksamhet, behov av skyddsåtgärder inom

- administrativ databehandlingsverksamhet
- processreglering
- lagerstyrning
- distribution

Det gäller således verksamhet

- som kan utgöra meningsfulla mål för dem som allvarligt vill störa samhället
- där sådana effekter kan bli resultatet redan av oavsiktliga handlingar eller ett tekniskt sammanbrott, vad orsaken därtill än må vara, och leda till att verksamheten endast svårligen eller inte alls kan upprätthållas därför att människor ersatts med teknik eller
- där lagrad information kan missbrukas till allvarligt men för samhället, verksamheten som sådan eller grupper av medborgare.

Det är emellertid mycket svårt att finna en lämplig gemensam nämnare som kan användas som hjälpmedel att sålla fram de skyddsvärda verksamheterna.

Trots svårigheterna bör man i vart fall hypotetiskt diskutera ett alternativ som innebär lagstiftning på sårbarhetsområdet inom såväl den offentliga som den enskilda sektorn och en myndighet som vakar över lagstiftningens efterlevnad. En sådan modell kan skisseras på följande sätt.

Med utgångspunkt från en likartad behandling av alla samhällsområden borde följande alternativ kunna prövas:

1. Administrativ databehandlingsverksamhet med undantag för personregistrering som med stöd av datakungörelsen (1973:291) och datainspektionens författningssamling bedrivs enligt det s k förenklade förfarandet.

2. Elektroniskt styrd industriell processreglering samt lagerhållnings- och distributionssystem hos s k K-företag.

Avgränsningen av den administrativa databehandlingen blir något för vid eftersom det sannolikt finns verksamhet som omfattar annat än personregistrering men som inte behöver åtgärdas från sårbarhetssynpunkt. Ett exempel kan vara vissa typer av bokföringsrutiner. Den myndighet som får ansvaret för normernas efterlevnad bör särskilt uppmärksamma detta och sedan viss tids erfarenhet vunnits föreslå ytterligare avgränsning. För att underlätta dess verksamhet att nå fram till rimliga avgränsningar bör finnas en allmän undantagsregel som gäller båda kategorierna 1 och 2. Genom en sådan regel bör det vara möjligt att undanta användningen av ADB-teknisk utrustning som med hänsyn till arten, användningsområdet eller omständigheterna i övrigt uppenbarligen saknar betydelse för samhällets sårbarhet.

För att genomgripande komma tillrätta med problemen skulle egentligen krävas en prövning av all inom en offentlig eller privat organisa-

tion bedriven databehandlingsverksamhet eller processreglering. Denna prövning borde gälla både existerande verksamhet och sådan som allteftersom tas i drift. Tillståndsprövningen borde således inte begränsas till den offentliga sektorn.

Till synes skulle en sådan ordning kunna kraftfullt förbättra den rådande situationen. Det måste i detta sammanhang dock beaktas att i dagens samhälle finns endast kvantitativt och kvalitativt begränsad kompetens att tillgå. Även om denna kompetens med nödvändighet på sikt bör och kan förstärkas blir det svårt att genomföra en detaljprövning. Det är bl a därför nödvändigt att begränsa tillståndstvånget.

Ett tillståndstvång koncentrerat till den offentliga sektorn blir väsentligen en rutin som drabbar kommunal och landstingskommunal verksamhet. Det kan nämligen förutsättas att på den statliga sektorn kommer de mera betydelsefulla verksamheterna att regleras genom beslut av regeringen eller riksdagen.

Mot bakgrund av det anförda kan enligt min mening ifrågasättas om man inte borde nöja sig med att ställa kraven på nödvändiga åtgärder i en lag om skydd för databehandlingsverksamhet m m och att uppdra åt någon myndighet att lämna råd och anvisningar samt övervaka lagens efterlevnad. Ett sådant alternativ borde närmare ha utretts före ett slutligt ställningstagande inom SÅRK. Emedan detta inte skett kan alternativet inte här redovisas i detalj. Jag vill dock något diskutera ett sådant alternativ.

I lagen borde krävas att ansvarig för administrativ databehandlingsverksamhet samt industriell processreglering, lagerhållning och distribution som nu är i fråga bör åläggas att vidta och ajourhålla sådana åtgärder för kapital-, funktions- och dataskydd som har förebyggande, rapporterande, begränsande och återställande effekt samt har betydelse mot katastrofhändelser. I detta sammanhang är utlandsberoendet av speciellt intresse.

Särskild betydelse för det förebyggande skyddet har katastrofplanering. Till det förebyggande funktionsskyddet hör den dokumentation som erfordras för att inom en för verksamheten rimlig tid (t ex cirka sex veckor) antingen återuppta driften efter driftavbrott eller att ta t ex manuella reservrutiner i bruk. Hit hör också personalplanering och bemanningsplan. Till katastrofplaneringen och det förebyggande kapitalskyddet hör att vidta erforderliga förberedelser för reservdelsförsörjning eller för att ta reservutrustning eller reservlokaler i drift. Rapporterande skydd innefattar sedvanliga inbrotts- och brandlarmanordningar m m men omfattar också sådana larm som utlöser dataskyddsåtgärder såsom undanförsel eller förstöring av maskinell utrustning och information. Loggning bör vara ett obligatorium och alla former av dataintrång eller försök eller förberedelse därtill bör anmälas till ansvarig myndighet.

I och för sig har under senare år vissa av dessa åtgärder på en del håll mer eller mindre framgångsrikt genomförts i olika sammanhang. Utredningsarbete har bedrivits av många och rapporter har framställts av bl a statskontoret eller av datortillverkare i samverkan bl a med datainspek-

tionen och statskontoret osv. Underlag för författningstext finns således och därför skall här endast några detaljer belysas ytterligare.

För berörd verksamhet är det nödvändigt att rutiner finns för undanförsel och förstöring av maskinell utrustning, dokumentation och, i förekommande fall, av lagrad information. Sådana rutiner finns i dag inte för all sådan verksamhet. Exempelvis kan på den privata sektorn finnas personinformation som utgör direkt kopia av information hos myndighet som är underkastad regler om undanförsel och förstöring. Samma regler bör gälla oavsett var informationen finns lagrad.

Till betydande del lagras reservdelar i dag utomlands. Detta förhållande är otillfredsställande. Därför bör vid anskaffning av hårdvaruutrustning i köpe- eller hyresavtal också träffas avtal om reservdelsförsörjning med leverantören. Denne bör i avtalet åläggas att inom riket hålla lager av reservdelar, avpassat med hänsyn till utrustningens beräknade livslängd. Detta torde inte behöva leda till drastiska merkostnader eftersom hårdvarupriset redan sjunkit markant och alltjämt fortsätter att sjunka.

Utlandsbearbetningar bör alltid föregås av utredning om alternativa bearbetningsmöjligheter inom landet. Härvid bör dras nytta av den myndighet som får ansvaret för sårbarhetsfrågorna. Denna bör skyndsamt skaffa sig överblick som medger rådgivning på detta område. I den mån resultatet blir att sådana möjligheter saknas bör med den som i utlandet tillhandahåller datorkraften träffas avtal av innehåll att samma skyddsåtgärder som gäller inom landet skall tillämpas. Utlandsbearbetningar bör således förutsätta en anmälan till och diskussion med den ansvariga myndigheten.

Dessa krav bör kunna anges i lag. Kraven bör vara uppfyllda innan verksamheten tas i drift. Detaljerna beträffande kraven bör anges närmare i en på lagen följande kungörelse och myndighetsförfattning. I lagen måste med nödvändighet kraven anges i ganska vida formuleringar som t ex att dokumentationen skall vara tillräckligt utförlig och ajourhållen för att kunna tjäna som underlag för en återuppbyggnad av verksamheten. Dataskyddet är ett typexempel på att i författning endast kan anges en katalog av alternativa åtgärder som kan bli aktuella eftersom miljön där verksamheten bedrivs och verksamhetens art ofta blir avgörande. Det kan t ex finnas skäl att välja mellan fysisk bevakning av lokalen eller låsanordningar osv.

De aktuella åtgärderna är av intresse både för den särskilda verksamheten som sådan hos myndigheter och företag men främst för samhället som helhet.

Det bör således bli fråga om en reglering av samma form som t ex bokföringslagens bestämmelser; den ansvarige ges ledning och bedömer i första hand själv hur flertalet av de i författningarna ställda kraven skall kunna uppfyllas i hans verksamhet. Enligt min mening går det att specificera kraven i sådan grad att risken för rättsosäkerhet i vart fall inte blir större än på många andra områden.

Det blir således inte fråga om någon tillståndsprövning. Lagstiftningens grundläggande betydelse blir dess funktion som underlag för rådgiv-

ning, när tveksamhet uppkommer om vilka åtgärder som är påkallade. Därutöver blir det fråga om tillsyn.

Lagen bör träda i kraft snarast möjligt dvs senast den 1 januari 1981. Verksamhet som dessförinnan har tagits ikraft bör senast den 1 juli 1984 ha anpassats till lagens krav. Hinder bör inte föreligga för att låta rådgivningen dessutom kunna omfatta så vitt skilda ting som lämplig lokalisering av databehandlingsverksamheten, olika former av koncentration, verksamhetens externa beroende, koordinatsättning, kryptering, filsplittring, liksom andra skyddsåtgärder som kan komma att utvecklas.

För att ge lagstiftningen erforderlig tyngd och tvinga ansvariga till att följa den bör uppdras åt den myndighet som tilldelas ansvaret för sårbarhetsfrågorna att utöva tillsyn över det aktuella området. I den mån någon uppenbarligen underlåter att uppfylla kraven på ett för hans verksamhet rimligt sätt bör finnas sedvanlig skala av sanktioner.

Även om en del av de berörda frågorna redan i dag faller på vissa olika myndigheter bör ansvaret för skyddet för databehandlingsverksamheten sammanföras till en enda myndighet med skyldighet att i förekommande fall samråda med övriga berörda och därmed också åstadkomma samordning. Behovet av en sådan nyordning är inte unikt för detta område.

Oavsett vilken metod som väljs kommer besvärliga avvägningsfrågor att uppkomma. Mot bakgrund härav samt de betydelsefulla samhällsintressen som berörs är det nödvändigt att den ansvariga myndigheten ges en beslutsfunktion, med bred sammansättning. Denna bör ha starkt parlamentariskt inslag.

Eftersom jag i likhet med övriga ledamöter anser att snara åtgärder krävs ansluter jag mig till kommitténs förslag. Det är viktigare att något görs åt problemen nu än att fortsatt utredning av nyanserade former av författningsreglering tillåts fördröja önskvärda åtgärder. På sikt bör dock här diskuterade rutiner kunna införas.

Bilaga Utkast till sårbarhetslag (SÅRL)

Inledande bestämmelser

1 § I denna lag avses med

register:	register, förteckning eller andra anteckningar som förs med hjälp av dator
personregister:	register, förteckning eller andra anteckningar som förs med hjälp av dator och som innehåller personuppgift som kan hänföras till den som avses med uppgiften
datoranvändare:	den som i sin verksamhet för egen räkning använder dator som hjälpmedel samt den som använder dator för att för annans räkning tillhandahålla datorkraft med därtill hörande tjänster (dataserviceföretag)

2 § Denna lag gäller användning av datorer och avser följande datoranvändare

1. myndigheter med undantag av sådana som tillhör försvarsmakten
2. statligt eller kommunalt ägda företag som tillhandahåller datorkraft med därtill hörande tjänster
3. annan datoranvändare dock inte myndighet som tillhör försvarsmakten, som inrättar och för personregister som omfattar hela eller stora delar av befolkningen i riket eller i övrigt ett stort antal personer eller omfattar uppgifter om persongrupper som kan vara av intresse för utländsk underrättelsetjänst
4. samt därutöver företag och organisationer som kan anses vara särskilt viktiga för landets försörjning.

Närmare föreskrifter rörande tillämpningen av punkten 4 meddelas av regeringen.

Tillstånd m m

3 § Myndighet, företag eller organisation som omfattas av lagen enligt 2 § 1, 2 och 3 får inte använda dator utan tillstånd av datainspektionen.

Första stycket gäller inte om användningen av dator beslutats av regeringen eller riksdagen. Före sådant beslut skall yttrande inhämtas från datainspektionen.

Första stycket gäller inte heller användning av dator som, med hänsyn till utrustningens art, användningsområde eller omständigheterna i övrigt, uppenbarligen inte kommer att medföra sårbarhetsrisker.

Närmare föreskrifter rörande tillämpningen av tredje stycket meddelas av regeringen eller av den myndighet regeringen bestämmer.

4 § Användning av dator enligt 2 § 4 skall anmälas till datainspektionen. Närmare föreskrifter om vad anmälan skall innehålla meddelas av regeringen.

5 § Datainspektionen skall meddela tillstånd till användning av dator om, med iakttagande av de föreskrifter som meddelas enligt 6 §, användningen kan anses godtagbar från sårbarhetssynpunkt.

Vid denna prövning skall särskilt beaktas registerinnehåll, datordriftens organisation, beroendet av andra datoranvändare samt beroendet av utlandet.

Föreligger särskilda skäl får datainspektionens tillstånd begränsas till viss tid.

6 § I samband med att tillstånd till att använda dator lämnas skall datainspektionen om det behövs för att minska sårbarheten meddela föreskrifter om

1. registerinnehåll vad gäller uppgifternas art och mängd samt beträffande personregister även personkretsen,
2. vilka bearbetningar som får göras och vilka uppgifter som får göras tillgängliga,
3. utlämnande och annan användning av uppgifter,
4. bevarande och gallring av uppgifter,
5. datordriftens organisation,
6. olika ADB-säkerhetsåtgärder,
7. reservrutiner, katastrofplaner och katastrofberedskap,
8. personalplanering och dokumentation,
9. i vad mån utlandsbearbetningar får ske.

Föreskrift om utlämnande av registeruppgift får inte inskränka myndighets skyldighet enligt tryckfrihetsförordningen.

7 § Bestämmelsen i 6 § om skyldighet för datainspektionen att meddela föreskrift gäller även i fråga om användning av dator som avses i 3 § andra stycket i den mån inte regeringen eller riksdagen har meddelat föreskrift i samma hänseende.

8 § Skall register som omfattas av lagen inte längre föras skall detta anmälas till datainspektionen. Inspektionen föreskriver i sådant fall hur det skall förfaras med registret.

Tillsyn m m

9 § Datainspektionen utövar tillsyn över att användning av dator inom det tillståndspliktiga området sker på ett från sårbarhetssynpunkt godtagbart sätt.

Tillsynen skall utövas så, att den inte vållar större kostnad eller olägenhet än nödvändigt.

10 § Datainspektionen har rätt att för tillsynen få tillträde till lokal där datordriften sker eller där dator eller utrustning eller upptagning för automatisk databehandling förvaras. Inspektionen har vidare rätt till handling som rör datordriften samt rätt att föranstalta om datorkörning.

11 § Ansvarig datoranvändare skall lämna datainspektionen de uppgifter om användningen som inspektionen begär för sin tillsyn.

12 § Om användning av dator inte sker på ett från sårbarhetssynpunkt godtagbart sätt får datainspektionen i mån av behov ändra föreskrift som tidigare meddelats eller meddela ny föreskrift i sådant avseende som anges i 6 §. I fråga om användning av dator som avses i 3 § andra stycket får datainspektionen vidtaga åtgärd som nu nämnts endast i den mån den ej står i strid med beslut av regeringen eller riksdagen.

Om det är oundgängligen nödvändigt för att uppnå en godtagbar säkerhetsnivå får datainspektionen återkalla meddelat tillstånd.

Straff m m

13 § Till böter eller fängelse i högst ett år dömes den som uppsåtligen eller av oaktsamhet

1. använder dator utan tillstånd enligt denna lag, när sådant erfordras,
2. använder dator utan att göra anmälan enligt 4 §, när sådan erfordras,
3. bryter mot föreskrift som meddelats enligt 6 §,
4. bryter mot 8 § eller
5. lämnar osann uppgift i tillståndsansökan, i anmälan eller i fall som avses i 11 §.

14 § Används dator utan tillstånd enligt denna lag, när sådant tillstånd erfordras, kan utrustning, programvara och register förverkas, om det inte är uppenbart obilligt.

15 § Om ansvarig datoranvändare underlåter att lämna tillträde till lokal eller tillgång till handling i fall som avses i 10 § eller att lämna uppgift enligt 11 §, får datainspektionen förelägga vite.

16 § Talan mot datainspektionens beslut föres hos regeringen genom besvär. Justitiekanslern får föra talan för att tillvarataga allmänna intressen.

Övergångsbestämmelser

Denna lag träder i kraft den 1 juli 1981.

För användning av dator som påbörjats före lagens ikraftträdande gäller lagen från och med den 1 juli 1986 om inte användningen dessförinnan undergår väsentliga förändringar, för vilket fall lagen tillämpas från tidpunkten för förändringen. För användning av dator som påbörjats

före lagens ikraftträdande behöver anmälan enligt 4 § ske endast i samband med väsentliga förändringar.

Datainspektionen får fr o m den 1 juli 1980 pröva ansökan om tillstånd samt meddela föreskrift såvitt avser tid efter utgången av juni 1981.

Användning av dator som påbörjats före lagens ikraftträdande och som inte undergått väsentliga förändringar får under förutsättning att ansökan om tillstånd görs före den 1 juli 1986 fortsätta utan tillstånd till dess ansökningen slutligen prövats.

Litteraturförteckning

Statens offentliga utredningar (SOU)

1972:47	Data och integritet
1974:10	Data och näringspolitik
1975:22	Lag om allmänna handlingar
1975:57	Varuförsörjning i kristid
1976:5	Säkerhetspolitik och totalförsvar
1976:12	Företagens uppgiftslämnande
1976:19	Den militära underrättelsetjänsten
1976:56 och 57	Fastighetsdata
1976:58	ADB och samordning
1976:68	Moderna arkivmedier
1977:1	Totalförsvaret 1977—82
1978:48	Konkurrens på lika villkor
1978:54	Personregister—Datorer—Integritet, översyn av datalagen
1979:69	Nya vyer. Datorer och nya massmedier — hot eller löfte?
1979:72	Rationalisering och ADB i statsförvaltningen

Propositioner

1973:33	med förslag till ändringar i tryckfrihetsförordningen och förslag till datalag m m
1973:37	med förslag till lagstiftning om åtgärder mot vissa våldsdåd med internationell bakgrund
1975:57	om ett nytt system för automatisk databehandling inom folkbokförings- och beskattningsområdet
1975:104	med förslag till bokföringslag
1976/77:27	om åtgärder för att begränsa möjligheterna att föra omfattande personregister
1976/77:138	om genomförande av den nya taxeringsorganisationen m m
1976/77:74	om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling
1977/78:38	om ändring i sekretesslagen m m
1978/79:109	om ändring i datalagen
1978/79:121	om användning av ADB i statsförvaltningen
1979/80:2	med förslag till sekretesslag m m

Utskottsbetänkanden

Justitieutskottet 1975/76:46 med anledning av proposition 1975/76:174 om ändring i brottsbalken (ang spioneribrottet m m)

Finansutskottet 1978/79:34 med anledning av proposition 1978/79:121 om användning av ADB i statsförvaltningen.

Motioner till riksdagen

1974:1 angående äganderätt till data m m

Departementspromemorior

Ds Kn 1976:1 och 2	ADB inom samhällsplaneringen
Ds Kn 1976:7	ADB i den regionala samhällsplaneringen
Ds Ju 1977:11	Handlingssekretess och tystnadsplikt
Ds I 1978:1	Swedish Reactor Safety Study
Ds B 1979:1	Datakonkurrens
Ds S 1979:4	ADB inom den allmänna försäkringen — på 1980-talet och därefter
Ds Ju 1979:6	Översyn av spioneribrottet m m

Försvarsdepartementet, SSLP, Påtryckningar och hot, Stockholm 1975

Försvarsdepartementet, SSLP, Telekommunikationerna, Stockholm 1976

Försvarsdepartementet, SSLP, Samhällets sårbarhet, Stockholm 1976

Litteratur

Abrams, D. Marshall, m fl: Tutorial on Computer Security and Integrity, IEEE Computer Society, Long Beach, Kalifornien 1977

An Analysis of Computer Security Safeguards For Detecting And Preventing Intentional Computer Misuse, SRI-rapport till National Bureau of Standards, Washington 1978

Anér, Kerstin: Datamakt, Gummesons, Falköping 1975

Bergqvist, Mats: Krig och surrogatkrig, Centralförbundet Folk och Försvar, Stockholm 1976

Björk, Lars-Eric, Saving, Jaak: Datorer på våra villkor, LiberLäromedel, Malmö 1975

Computer Security In Federal Programs, Committee On Government Operations, United States Senate, Washington 1977

Eriksson Allan, Freese Jan, Johansson Lennart: Datorerna och samhällets sårbarhet, Centralförbundet Folk och Försvar, Stockholm 1976

Framsteg inom forskning och teknik 1973, Ingenjörsvetenskapsakademins meddelande 180, Stockholm 1973

Freese, Jan: Data och livskvalitet, Liber, Stockholm 1976

Håkansson, Bertil: Den mångsidiga mikrodatorn, Svenska Ingenjörsamfundet/Ingenjörsförlaget, Stockholm 1976
Kullberg Gunnar, Eriksson Sven-Åke, Johannesson Dan, Lumsden Kenth: Samordnad Datorstödd Produktion — verkstadsindustrins framtid, Ingenjörsförslaget, Stockholm 1976
Palme, Jacob: Datorers betydelse för samhällets och människornas sårbarhet, FOA-rapport, mars 1979
Parker Donn B: Crime By Computer, Charles Scribner's Sons, New York 1976
Parker Donn B, Nycum Susan, Oüra S Stephen: Computer Abuse, Stanford Research Institute, 1973
Problems Associated With Computer Technologi In Federal Programs And Private Industry, Computer Abuses, Committee On Government Operations United States Senate, Washington 1976
Wermdalen, Hans: Företagen och Terrorismen, Stockholm 1977
Where next for Computer Security, The National Computing Centre Limited, England 1974
2002: Britain Plus 25, The Hanley Centre for Forecasting, London 1977

Övrigt material

ADB och arbetskraften — verkstadsindustrin, information i prognosfrågor (SCB) nr 1973:8
ADB och arbetskraften — en delfistudie, information i prognosfrågor nr 1974:2
ADB och arbetskraften — utvecklingen och konsekvenserna av datorteknikens tillämpning i Sverige. Ett scenarioförsök, information i prognosfrågor nr 1974:3
ADB och arbetskraften — industrins ADB-förhållanden 1972, information i prognosfrågor nr 1975:1
ADB och arbetskraften — en slutrapport, information i prognosfrågor nr 1977:2
ADB och arbetskraften — varuhandelns ADB-förhållanden, promemoria från SCB nr 1976:11
ADB och arbetskraften — några ADB-system inom den statliga sektorn och deras effekter, promemoria från SCB nr 1977:1
ADB och arbetskraften — ADB-förhållanden inom landstingens verksamhetsområde, promemoria från SCB nr 1977:2
ADB och informationssystemsäkerhet i försvaret — en förstudie, FRI rapport 4.77-8901
ADB-system inom allmän försäkring m m 1976—1980 och därefter, rapport från statskontoret 1976-03-29 (1976:13)
ADB-säkerhet i dag och i morgon, dokumentation från en konferens om ADB-säkerhet november 1976, Nynäshamn
ADB-säkerhet; Kontroller vid ADB, rapport nr 1979:11 från statskontoret
ADB-teknik i ett tioårsperspektiv, FRI-rapport 9/73-3101

Anvisningar för planläggning av informationsbehandling i krig (Anv Infob K), ÖEF 1975
Civila statliga myndigheters databehandling i krig, FRI-rapport 71-8902
Datamarknaden inför 1980-talet, SIND 1978:1
Dataskydd, rapport 1975:9 och 1976:38 från statskontoret
Datasäkerhet. Hot och brister vid datordrift, rapport från en hotstudie planerad av statskontoret och IBM Svenska AB
Datasäkerhetshandboken, IBM Svenska AB
Datateknik. Miljöstudie 1980—85, rapport av Statskonsult AB för datasamordningskommittén och dataindustriutredningen, Stockholm 1974
Data under beredskap och krig (DBK 71), utredning 1972-04-13 av ÖEF.
Datorer på människans villkor, förslag till socialdemokratiskt program för datapolitiken
Den norska propositionen med förslag till lag om personregister m m, Ot prp nr 2 (1977—78)
The fire and after the fire, broschyr utgiven av IBM
Föreskrifter och anvisningar till datalagen 1975-08-20, datainspektionen
Kapitalskydd, rapport 1976:39 från statskontoret
Katastrofplanering — en kartläggning, rapport 1977-06-28 av Statskonsult AB
Konferensdokumentation från Norddata 1976 (vol 1—3) och 1977 (vol 1—2)
Kvalitetsskydd av data, utredning av statskontoret och SCB, Liber, Stockholm 1977
Revisionsrapport av RRV 1978-02-17. Tio myndigheters ADB-verksamhet, styrning, kostnader m m
Security in the EDP Environment, kanadensisk rapport från januari 1979
Storstörningar i distributionsnät i tätorter, Svenska elverksföreningen 1974
The Usage of International Data Networks in Europe. Rapport 1978-04-01 av Logica för OECD
Artiklar i fack- och dagspress

Statens offentliga utredningar 1979

Kronologisk förteckning

1. Utbyggt skydd mot höga vård- och läkemedelskostnader. S.
2. Naturmedel för injektion. S.
3. Regional laboratorieverksamhet. Jo.
4. Avskildhet och gemenskap inom kriminalvården. Ju.
5. Konsumentinflytande genom insyn? H.
6. Polisen. Ju.
7. Tandvården i början av 80-talet. S.
8. Löntagarna och kapitaltillväxten 1. Löntagarfonder – bakgrund och problemanalys. E.
9. Löntagarna och kapitaltillväxten 2. Den svenska förmögenhetsfördelningens utveckling. Löntagarfonder och aktiemarknaden-en introduktion. Internationella koncerner och löntagarfonder. E.
10. Löntagarna och kapitaltillväxten 3. Löner, lönsamhet och soliditet i svenska industriföretag. Vinstbegreppet. Den lokala lönebildningen och företagets vinster – en preliminär analys. E.
11. Löntagarna och kapitaltillväxten 4. Lantbrukskooperationen – ideologi och verklighet. E.
12. Svenska kyrkans gudstjänst. Band 4. Evangelieboken. Kn.
13. Konkurs och rätten att idka näring. Ju.
14. Naturvård och täktverksamhet. Jo.
15. Naturvård och täktverksamhet. Bilagor. Jo.
16. Ökad sysselsättning. Finansiella effekter i offentliga sektorn. A.
17. Kulturhistorisk bebyggelse – värd att vårda. U.
18. Museijärnvägar. U.
19. Jaktvårdsområden. Jo.
20. Anhöriga. S.
21. Plötslig och oväntad död – anhörigas sjuklighet och psykiska reaktioner. S.
22. Barn och döden. S.
23. Avgifter i staten – nuläge och utvecklingsmöjligheter. B.
24. Sysselsättningspolitik för arbete åt alla. A.
25. Nya namnregler. Ju.
26. Sjukvårdens inre organisation – en idépromemoria. S.
27. Sysselsättningspolitik för arbete åt alla. Bilagedel. A.
28. Barnolycksfall. S.
29. Lotterier och spel. H.
30. Lotterier och spel. Bilagor. H.
31. Bättre kontakter mellan enskilda och myndigheter. Kn.
32. Fastighetstaxering 81. B.
33. Fastighetstaxering 81. Bilagor. B.
34. Bilarna och luftföroreningarna. Jo.
35. Rationellare girohantering. E.
36. Konsumenttjänstlag. Ju.
37. Aktivt boende. Bo.
38. Lagerstöd. A.
39. Vattenkraft och miljö 4. Bo.
40. Malmer och metaller. I.
41. Barnen i framtiden. S.
42. Vår säkerhetspolitik. Fö.
43. Ren tur. Program för miljösäkra sjötransporter. Jo.
44. Ren tur. Program för miljösäkra sjötransporter. Bilagor 1–8. Jo.
45. Ren tur. Program för miljösäkra sjötransporter. Bilagor 9–13. Jo.
46. Koncernbegreppet m. m. Ju.
47. Dokumentation och statistik om högskoleutbildning. U.
48. Arbetstiderna inför 80-talet. A.
49. Grundlagsskyddad yttrandefrihet. Ju.
50. Huvudmannaskapet för specialskolan. U.
51. Öst Ekonomiska Byrån. H.
52. Viltskador. Jo.
53. Nytt skördeskadeskydd. Jo.
54. Hushållning med mark och vatten 2. Del I. Överväganden. Bo.
55. Hushållning med mark och vatten 2. Del II. Bakgrundsbeskrivning. Bo.
56. Steg på väg. . . A.
57. Barnomsorg – behov, efterfrågan, planeringsunderlag. S.
58. Barnomsorg. Redovisning av särskilda undersökningar. S.
59. I livets slutskede. S.
60. Bidrag till folkrörelser. Kn.
61. Förnyelse genom omprövning. B.
62. Kooperationen i Sverige. I.
63. Barnets rätt 2. Om föräldraansvar m. m. Ju.
64. Ny utlänningslag A.
65. Ny plan- och bygglag. Del I. Bo.
66. Ny plan- och bygglag. Del II. Bo.
67. Svensk sjöfartspolitik. K.
68. De allmänna advokatbyråerna. Ju.
69. Nya vyer. Datorer och nya massmedier – hot eller löften. U.
70. Tandvård i fred för värnpliktiga. Fö.
71. Handläggningen av anmälningar mot polispersonal. Ju.
72. Rationalisering och ADB i statsförvaltningen. B.
73. Krigets lagar. Fö.
74. Serviceföretagen–vägar till utveckling. H.
75. Polisen i totalförsvaret. Ju.
76. Ny hemförsäljningslag. Ju.
77. Hemslöjd-kulturarbete, produktion, sysselsättning. I.
78. Mål och medel för hälso- och sjukvården. S.
79. Produktansvar 2. Produktansvarslag. Ju.
80. Prognoser och arbetsmarknadsstatistik för högskolan. U.
81. Fastighetstaxering -81. Industribyggnader. B.
82. Personell assistans för handikappade. U.
83. Om vi avvecklar kärnkraften. I.
84. Lekmän i försvaret. Fö.
85. Folkbildning för 80-talet. U.
86. Säker kärnkraft? I.
87. Chanser till utveckling. A.
88. Städbranschen. H.
89. Kvinnors arbete. A.
90. Regional arbetsfördelning inom industrin. I.
91. Företags obestånd. B.
92. Komvux och studieförbund. U.
93. ADB och samhällets sårbarhet. Fö.

Statens offentliga utredningar 1979
Systematisk förteckning

Justitiedepartementet

Avskildhet och gemenskap inom kriminalvården. [4]
1975 års polisutredning. 1. Polisen. [6] 2. Polisen i totalförsvaret. [75]
Konkurs och rätten att idka näring. [13]
Nya namnregler. [25]
Konsumenttjänstlag. [36]
Koncernbegreppet m. m. [46]
Grundlagsskyddad yttrandefrihet. [49]
Barnets rätt 2. Om föräldraansvar m. m. [63]
De allmänna advokatbyråerna. [68]
Handläggningen av anmälningar mot polispersonal. [71]
Ny hemförsäljningslag. [76]
Produktansvar 2. Produktansvarslag. [79]

Försvarsdepartementet

Vår säkerhetspolitik. [42]
Tandvård i fred för värnpliktiga. [70]
Krigets lagar. [73]
Lekmän i försvaret. [84]
ADB och samhällets sårbarhet.[93]

Socialdepartementet

Utbyggt skydd mot höga vård- och läkemedelskostnader. [1]
Naturmedel för injektion. [2]
Tandvården i början av 80-talet. [7]
Utredningen rörande vissa frågor beträffande sjukvård i livets slutskede. 1. Anhöriga. [20] 2. Plötslig och oväntad död – anhörigas sjuklighet och psykiska reaktioner. [21] 3. Barn och döden. [22] 4. I livets slutskede. [59]
Sjukvårdens inre organisation – en idépromemoria. [26]
Barnolycksfall. [28]
Barnen i framtiden. [41]
Planeringsgruppen för barnomsorg. 1. Barnomsorg – behov, efterfrågan, planeringsunderlag. [57] 2. Barnomsorg. Redovisning av särskilda undersökningar. [58]
Mål och medel för hälso- och sjukvården. [78]

Kommunikationsdepartementet

Svensk sjöfartspolitik. [67]

Ekonomidepartementet

Utredningen om löntagarna och kapitaltillväxten. 1. Löntagarna och kapitaltillväxten 1. Löntagarfonder-bakgrund och problemanalys. [8] 2. Löntagarna och kapitaltillväxten 2. Den svenska förmögenhetsfördelningens utveckling. Löntagarfonder och aktiemarknaden- en introduktion. Internationella koncerner och löntagarfonder. [9] 3. Löntagarna och kapitaltillväxten 3. Löner, lönsamhet och soliditet i svenska industriföretag. Vinstbegreppet. Den lokala lönebildningen och företagets vinster – en preliminär analys. [10] 4. Löntagarna och kapitaltillväxten 4. Lantbrukskooperationen – ideologi och verklighet. [11]
Rationellare girohantering. [35]

Budgetdepartementet

Avgifter i staten – nuläge och utvecklingsmöjligheter. [23]
1976 års fastighetstaxeringskommitté. 1. Fastighetstaxering 81. [32] 2. Fastighetstaxering 81. Bilagor. [33] 3. Fastighetstaxering -81. Industribyggnader. [81].
Förnyelse genom omprövning. [61]
Rationaliseringar och ADB i statsförvaltningen. [72]
Företags obestånd. [91]

Utbildningsdepartementet

Kulturhistorisk bebyggelse – värd att vårda. [17]
Museijärnvägar. [18]
Utredningen om studiedokumentation och statistik för högskolan. 1. Dokumentation och statistik om högskoleutbildning. [47]
2. Prognoser och arbetsmarknadsstatistik för högskolan. [80]
Integrationsutredningen. 1. Huvudmannaskapet för specialskolan. [50] 2. Personell assistans för handikappade. [82]
Nya vyer. Datorer och nya massmedier – hot eller löfte. [69]
Folkbildning för 80-talet. [85]
Komvux och studieförbund. [92]

Jordbruksdepartementet

Regional laboratorieverksamhet. [3]
Naturvårdskommittén. 1. Naturvård och täktverksamhet. [14] 2. Naturvård och täktverksamhet. Bilagor. [15]
Jakt- och viltvårdsberedningen. 1. Jaktvårdsområden. [19] 2. Viltskador. [52]
Bilarna och luftföroreningarna. [34]
Miljörisker vid sjötransporter. 1. Ren tur. Program för miljösäkra sjötransporter. [43] 2. Ren tur. Program för miljösäkra sjötransporter. Bilagor 1–8. [44] 3. Ren tur. Program för miljösäkra sjötransporter. Bilagor 9–13. [45]
Nytt skördeskadeskydd. [53]

Handelsdepartementet

Konsumentinflytande genom insyn? [5]
Lotteriutredningen. 1. Lotterier och spel. [29] 2. Lotterier och spel. Bilagor. [30]
Öst Ekonomiska Byrån. [51]
Serviceföretagen–vägar till utveckling. [74]
Städbranschen. [88]

Arbetsmarknadsdepartementet

Sysselsättningsutredningen. 1. Ökad sysselsättning. Finansiella effekter i offentliga sektorn. [16] 2. Sysselsättningspolitik för arbete åt alla. [24] 3. Sysselsättningspolitik för arbete åt alla. Bilagedel. [27]
Lagerstöd. [38]
Arbetstiderna inför 80-talet. [48]
Jämställdhetskommittén. 1. Steg på väg... [56] 2. Chanser till utveckling. [87] 3. Kvinnors arbete. [89]
Ny utlänningslag. [64]

Bostadsdepartementet

Aktivt boende. [37]
Vattenkraft och miljö 4. [39]
Hushållning med mark och vatten 2. Del I. Överväganden. [54]
Hushållning med mark och vatten 2. Del II. Bakgrundsbeskrivning. [55]
PBL-utredningen. 1. Ny plan- och bygglag. Del I. [65] 2. Ny plan- och bygglag. Del II. [66]

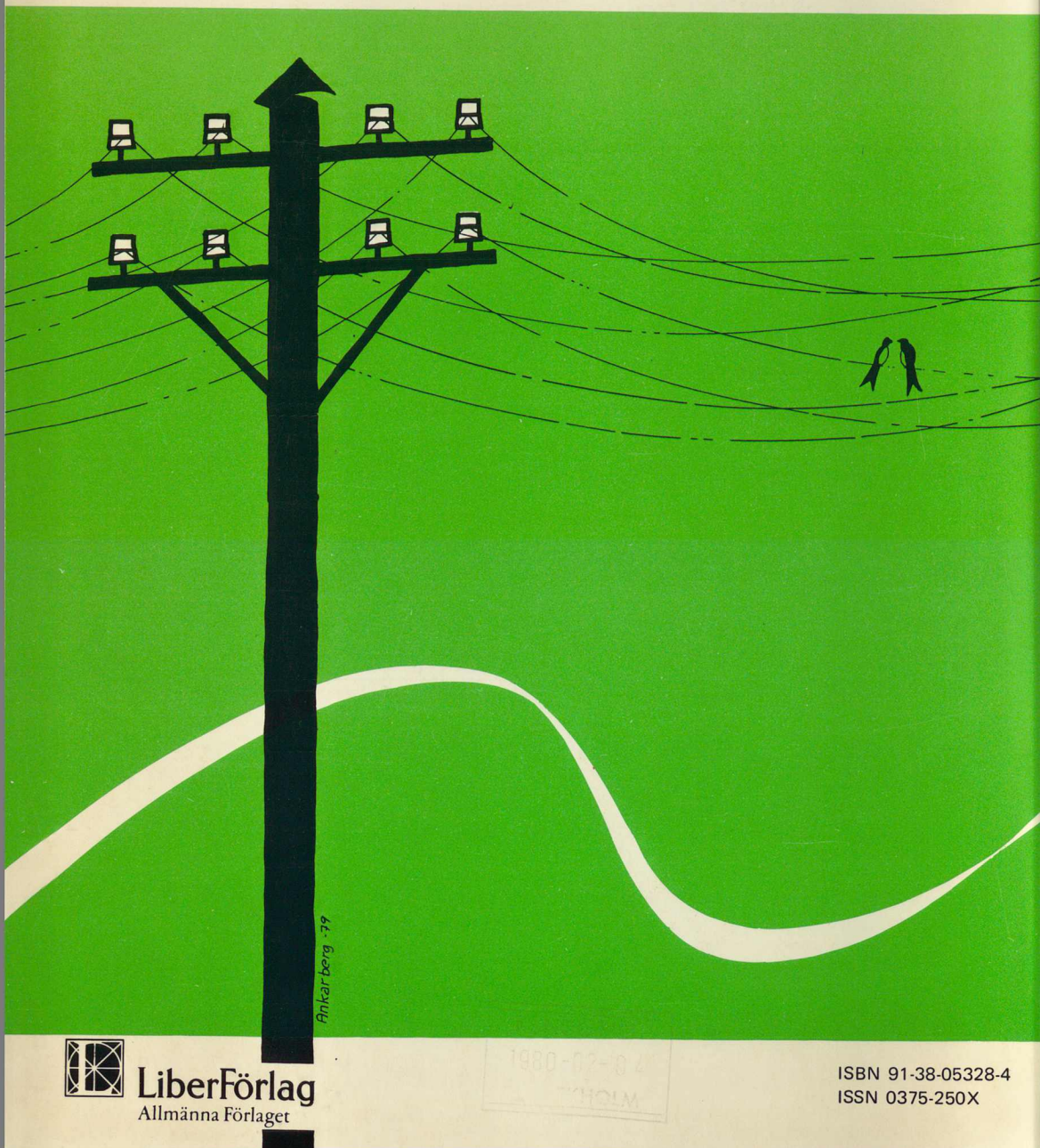
Industridepartementet

Malmer och metaller. [40]
Kooperationen i Sverige. [62]
Hemslöjd-kulturarbete, produktion, sysselsättning. [77]
Om vi avvecklar kärnkraften. [83]
Säker kärnkraft? [86]
Regional arbetsfördelning inom industrin. [90]

Kommundepartementet

Svenska kyrkans gudstjänst. Band 4. Evangelieboken. [12]
Bättre kontakter mellan enskilda och myndigheter. [31]
Bidrag till folkrörelser. [60]

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



LiberFörlag
Allmänna Förlaget

ISBN 91-38-05328-4
ISSN 0375-250X