

7 Strategi för ökad IT-säkerhet och skydd mot informationsoperationer

7.1 Bakgrund

7.1.1 Samhällets beroende av informationsteknik (IT)

Utvecklingen inom informationsteknik (IT), dvs. teknik för insamling, lagring, bearbetning och överföring av information med elektroniska medel, har på kort tid förändrat samhället. IT har blivit ett bekvämt hjälpmedel i många olika sammanhang och utgör grunden för teknik som var svår att föreställa sig för bara något decennium sedan. De positiva effekterna berör de allra flesta i samhället från privatpersoner till näringsliv och offentlig verksamhet. Det är viktigt att denna utveckling kan fortsätta för att även i framtiden bidra till frihet och ökade möjligheter.

En annan sida av utvecklingen är att samhället har blivit starkt beroende av IT. IT har blivit den viktigaste komponenten för informationsförsörjning, oavsett om det gäller information till privatpersoner, företagsinformation, teknisk information till styrsystem för andra teknikområden, eller någon annan typ av information. Information är en av de mest värdefulla tillgångarna i dagens samhälle. Den behöver skyddas likaväl som de fysiska tillgångarna. Viktiga samhällsfunktioner kan bli svårt störda, med i värsta fall katastrofala följder, om deras IT-stöd skulle störas eller slås ut. IT är i sig beroende av områdena elförsörjning och telekommunikationer för sin funktion (telekommunikationer kan med ett visst synsätt även betraktas som en del av IT), men IT utgör ändå något väsentligt mer än dessa båda områden tillsammans. Det är därför motiverat att betrakta IT som ett separat men samtidigt tvärsektorielt område som behöver ägnas särskild uppmärksamhet ur krishanteringsens alla aspekter.

Mot bakgrund av ovanstående finner utredningen det lämpligt att betrakta många av samhällets IT-komponenter som delar i en IT-infrastruktur. De delar som ingår är sådana som kan kommunicera genom något yttre nätverk, t.ex. Internet. Däremot ingår inte fristående datorer eller interna nätverk utan externa förbindelser. Men när en dator genom ett modem ansluts till omvärlden är den att betrakta som en del av det yttre nätverket och därmed en del av samhällets IT-infrastruktur. Se avsnitten 6.1.1 och 6.4.

IT är ett globalt område. Med Internet får man kontakt med organisationer och personer på andra sidan jordklotet lika enkelt som om de befann sig i en omedelbar geografisk närhet. Med den gränslöshet som IT-området präglas av, följer ett starkare behov av internationellt samarbete jämfört med andra områden, inte minst vad gäller IT-säkerhet och krishantering.

Tempot i utvecklingen på IT-området är mycket högt, vilket i grunden är positivt. Detta medför dock att nya produkter med täta mellanrum kommer ut på marknaden utan att de säkerhetsmässiga följderna på förhand är kända. Ur marknadens perspektiv kan detta te sig som en nödvändighet. Marknaden efterfrågar en ständigt utökad funktionalitet. Efterfrågan på IT-säkerhet är inte alls lika stor. IT-företagen måste tillgodose marknadens behov, och helst även skapa nya, för att inte snabbt slås ut. Så länge inte IT-säkerhet efterfrågas av marknaden i samma omfattning som funktionalitet, kommer denna att förbli sekundär.

Ser man till samhällets behov av skydd är detta ett problem. Kopplat till samhällets starka IT-beroende utgör bristande IT-säkerhet en potentiellt mycket stor sårbarhet. I och med att inte bara näringslivet utan hela samhället kan påverkas av de följder som kan uppstå p.g.a. bristande IT-säkerhet, kan samhället inte enbart förlita sig på att marknaden kommer att lösa problemen. Den offentliga sektorn med staten i spetsen måste enligt utredningens uppfattning ta ett stort ansvar och tillsammans med näringslivet agera kraftfullt för ökad IT-säkerhet. Staten måste därmed vidta ett antal åtgärder för att tillgodose samhällets behov av IT-säkerhet på de områden där inte marknaden till alla delar kan hantera problemen.

Avsnitt 7.2 är utredningens förslag till övergripande strategi för samhällets hantering av IT-säkerhet. Strategin bygger på propositionen *Ett informationssamhälle för alla*.¹ Avsnittet innehåller inga egentliga förslag, utan skall ses som en bakgrund till de efterföl-

¹ Prop. 1999/2000:86, bet. 1999/2000:TU9, rskr. 1999/2000:256

jande avsnitten. För att symboliskt markera avsnittets strategiska prägel och att det därmed skiljer sig från de övriga avsnitten ligger en särskild kantlinje i vänstermarginalen.

Utredningen föreslår att följande statliga funktioner inrättas: ett tvärsektoriellt samordningsorgan, en utpekad myndighet med övergripande ansvar för samhällets IT-säkerhet, en teknikkompetensfunktion, en IT-incidenthanteringsfunktion och en omvärldsanalysfunktion. Utredningens förslag till hur dessa funktioner skall arbeta återfinns i avsnitten 7.3–7.6.

En viktig förebyggande och förtroendeskapande åtgärd är att evaluera och certifiera säkerhet i IT-produkter. Utredningen finner det väsentligt att Sverige etablerar ett system för evaluering och certifiering, liksom att Sverige ansluter sig till den internationella överenskommelse mellan högt utvecklade länder om att ömsesidigt erkänna varandras utfärdade certifikat. Detta diskuteras närmare i avsnitt 7.7.

7.1.2 Vissa begrepp

Det finns många begrepp med snarlik innebörd, där det är oklart vari skillnaden består. IT-säkerhet och informationssäkerhet är två sådana begrepp. Informationssäkerhet är det övergripande begreppet, vilket omfattar IT-säkerhet och administrativ säkerhet som är relaterad till hantering av information i olika verksamheter. IT-säkerhet är skydd av information i informationsbehandlande tekniska system, vilket kan delas upp i datasäkerhet (ADB-säkerhet) och kommunikationssäkerhet. Administrativ säkerhet avser regler för personal, säkerhetsklassning av information, m.m. Begreppen är definierade i Informationstekniska standardiseringens (ITS) rapport *Terminologi för Informationssäkerhet*.²

Informationsoperationer och informationskrigföring är två andra begrepp som ligger nära varandra. Informationsoperationer (IO) är det övergripande begreppet, vilket är samlade och samordnade åtgärder i fred, kris och krig till stöd för ekonomiska, politiska eller militära mål genom att påverka eller utnyttja en motståndares eller annan aktörs information och informationssystem och samtidigt skydda egen information och egna informationssystem. Detta benämndes förr informationskrigföring (Information Warfare, IW), men p.g.a. de felaktiga associationer som ledet "krigföring" fört med sig, har informationskrigföring övergått till

² Rapport ITS 6, mars 1994

att beteckna den delmängd av informationsoperationer som bedrivs i kris och krig. Informationsoperationer behöver dock inte alls ha någon koppling till krig eller förberedelser för krig. En aktör kan välja att använda informationsoperationer för att uppnå sina syften utan att ha några som helst avsikter att övergå till väpnat angrepp. Därmed är skydd mot informationsoperationer en uppgift även för det civila samhället.

De defensiva aspekterna av informationsoperationer kallas informationssäkring (Information Assurance, IA), vilket innebär skydd av den egna informationen och de egna informationssystemen mot en angripares offensiva informationsoperationer. En skillnad mellan informationssäkring och informationssäkerhet är i vilket perspektiv man ser problemet. I informationssäkerhet har man valt ett nerifrån och upp-perspektiv med tekniken som kärna och administrativ säkerhet som ett viktigt komplement. I informationssäkring har man i stället valt ett uppifrån och ner-perspektiv med säkerhets- och försvarspolitik för ögonen, där helhetssynen är viktigare än de tekniska detaljerna. Det kan diskuteras på vilket sätt valet av perspektiv påverkar innehållet i begreppen och vilka skillnaderna blir i de praktiska åtgärderna som vidtas. Oavsett hur man ser på detta står det klart att IT-säkerhet är en grund för såväl informationssäkring som informationssäkerhet, och att beröringsytorna mellan IT-säkerhet, informationssäkerhet, informationssäkring, informationsoperationer och informationskrigföring är så stora att en nationell strategi måste beakta dessa frågor i ett sammanhang. Detta har också regeringen framhållit i propositionen *Ett informationssamhälle för alla*.³

Dagens hotbild avseende informationsoperationer mot Sverige är svårbedömd. Inga allvarliga incidenter har inträffat som skulle tyda på att en angripare med samlade och samordnade medel söker påverka svenska informationssystem på bred front. Detta behöver dock inte betyda att hotbilden inte existerar vare sig nu eller i framtiden. Aktörer, t.ex. stater, kan bygga upp en kapacitet att utföra offensiva informationsoperationer betydligt mer obemärkt och till en betydligt lägre kostnad än de kan bygga upp en motsvarande offensiv militär kapacitet. Dessutom saknar geografiska avstånd betydelse.

Även om sannolikheten för ett informationsoperationsangrepp mot Sverige med omfattande, allvarliga konsekvenser är svårbedömd, är konsekvensutfallet av en sådan magnitud att samhället

³ Prop. 1999/2000:86, bet. 1999/2000:TU9, rskr. 1999/2000:256

enligt utredningens uppfattning knappast kan negligera denna typ av risk. Ett osannolikt men inte orealistiskt exempel, utgående från en verklig händelse, kan illustrera denna risk. Den verkliga händelsen är att den 29 och 30 januari 2001 utfärdade det amerikanska företaget Verisign av misstag två certifikat⁴ utställda på Microsoft till en okänd person. Med dessa certifikat kan den okända personen sprida program som "bevisligen" är producerade av Microsoft. Vad dessa program gör vet ingen.

I det hypotetiska fallet är en angripare, som kan vara t.ex. en maffiaorganisation eller en illasinnad nation, den okända mottagaren, som dessutom utan att det upptäckts lyckats erhålla fler falska certifikat. Angriparen har lyckats placera programmen tillgängliga från en webbsida som ser ut att vara Microsofts. Programmen ser ut som om de reparerar säkerhetsbrister i Windows NT. Sådana program hämtar systemförvaltare regelbundet. Programmen gör visserligen det de lovar, men öppnar dessutom en tillfällig bakdörr och skickar ett meddelande till angriparen var de har installerats. Angriparen går då in genom de tillfälliga bakdörrarna, etablerar permanenta bakdörrar, byter ut de felaktiga programmen mot äkta vara och avslutar med att städa alla övriga spår. Därigenom har angriparen fått kontroll över samtliga system där de falska programmen installerats. Genom andra metoder än denna har angriparen även lyckats få motsvarande kontroll över ett stort antal andra system, varav flera är centrala i samhällsviktiga funktioner. Detta upptäcks inte eftersom angriparen inte avser att utnyttja kontrollen förrän långt senare samlat och samordnat. Angriparen kan därmed samtidigt allvarligt störa eller slå ut flera centrala funktioner i samhället såsom politisk ledning, teleföretag, banker osv. Genom det samtidiga förloppet är det inte säkert att det går att reparera eller ens upptäcka grundproblemet innan samhället har tvingats till eftergifter för angriparen eller i värsta fall helt kollapsat. Exemplet visar att konsekvenserna av ett litet misstag kan bli så stora att samhället måste ha en möjlighet att hantera denna typ av problem även om sannolikheten att de skall inträffa är liten.

⁴ Detta slags certifikat skall inte blandas samman med de certifikat för IT-produkter som diskuteras i avsnitten 7.4.5 och 7.7

7.1.3 Tidigare utredningar

Två statliga uppdrag har tidigare berört IT-säkerhet i ett helhetsperspektiv. *Arbetsgruppen för skydd mot informationskrigföring* (AgIW) presenterade 19 augusti 1998 i sin Rapport 2⁵ en strategi och ansvarsfördelning för skydd mot informationsoperationer (då benämnt informationskrigföring) med tio förslag:

En samordningsgrupp på hög nivå inom Regeringskansliet

En ny nationell IO-samordning inom Överstyrelsen för civil beredskap (ÖCB)

En s.k. StatsCERT under Post- och telestyrelsen (PTS) med stöd av Rikspolisstyrelsen (RPS)

Inrättande av en statistikenhet i dialog med Näringslivets säkerhetsdelegation (NSD)

Rapporteringsplikt för IT-relaterade incidenter inom statsförvaltningen

Försvarsmaktens mandat beträffande signalskyddstjänsten gentemot totalförsvaret – vilket förvaltas av TSA – vidgas till att även omfatta civila informationssystem av betydelse för totalförsvaret

En aktiv IT-kontrollfunktion för statsförvaltningen med Försvarsmakten som bas

Författningsändringar i datalagen m.m. initieras snarast

Mediebevakning på IT-området

Förändrade samverkansformer, delgivning, utbildning m.m. på underrättelseområdet vad avser IO-information

Dessa förslag behandlades av regeringen i propositionen Förändrad omvärld – omdanat försvar.⁶

PTS fick senare, som följd av AgIW:s förslag, i uppdrag att utreda förutsättningarna för att inrätta en särskild funktion för IT-incidenthantering. I en rapport daterad 28 november 2000 presenterade PTS sina överväganden och förslag. Utredningen kommenterar denna rapport i avsnitt 7.5.

Det andra övergripande uppdraget hade *Statskontoret*, som 24 juni 1998 presenterade sin rapport *Sammanhållen strategi för samhällets IT-säkerhet*.⁷ Detta uppdrag utfördes vid samma tid som AgIW utförde sitt uppdrag. AgIW och Statskontoret hade mellan sig dragit skiljelinjen så att Statskontoret inriktade sig mot hotbil-

⁵ Öppet utdrag ur hemligstämplad rapport 29 maj 1998, FO98 1297/MIL

⁶ Prop. 1998/99:74

⁷ Statskontoret 1998:18

den från enskilda personer upp till organisationer och företag i fredstid, medan AgIW hade hela hotbilden i kris och krig samt hotbilden stater och pakter i fredstid. Resultaten av de båda uppdragen förete stora likheter, med förslag som i stora drag stämmer överens med varandra. Även Statskontoret lade förslagen om att ÖCB skall ges en samordnande roll och att lagstiftningen skall ses över. Statskontoret föreslog också en statistikfunktion och en statlig incidenthantering. Statskontoret indikerade därvid att man borde överväga att göra rapporteringen obligatorisk för statliga myndigheter. Vidare föreslog Statskontoret att PTS skulle ges i uppdrag att ta initiativ till att åtgärder snarast vidtas för att erhålla en säkrare infrastruktur för Internet i Sverige. PTS fick i regleringsbrevet år 2000 av regeringen i uppdrag att utreda möjligheterna vidare. PTS redovisade 31 maj 2000 sina förslag till åtgärder i rapporten *Drift av Internet i Sverige oberoende av funktioner utomlands*.⁸ I regleringsbrevet år 2001 har PTS fått tre uppdrag som följer på denna rapport.

Statskontorets förslag behandlades av regeringen i propositionen *Ett informationssamhälle för alla*.⁹ I denna proposition gjorde regeringen bedömningen att en tvärspektoriell samordning för IT-säkerhet och skydd mot informationskrigföring bör utformas. Det ingår i Sårbarhets- och säkerhetsutredningens direktiv att föreslå hur utformningen skall göras. Regeringen gjorde vidare bedömningen att för den närmaste framtiden bör tre områden prioriteras: skydd mot informationsoperationer, ett säkrare Internet samt elektroniska signaturer och annan säkerhetsteknik.

Utöver de två nämnda övergripande statliga uppdragen, fick företaget Mandator Sverige AB (numera Cell Network AB) 1999 i uppdrag från Forsvarsdepartementet att bidra till ökad förståelse för informationsoperationer och strategiskt nationellt IT-skydd. Resultatet blev en rapport 21 december 1999 *Nationella strukturer för skydd mot informationsoperationer*.¹⁰ Mandator fann att ett antal funktioner behöver inrättas: en statistikfunktion, en hjälpfunktion, en analysfunktion, en IT-säkerhetsfunktion och en aktiv IT-kontrollfunktion.

⁸ PTS dnr 00-8824

⁹ Prop. 1999/2000:86, bet. 1999/2000:TU9, rskr. 1999/2000:256

¹⁰ Fö. 1999/3025/EC/RC

7.2 Vision och strategi

7.2.1 Vision: Sverige skall vara ett föredöme inom IT-säkerhet

En strategi för IT-säkerhet kopplad till informationssäkerhet och till den nationella informationsinfrastrukturens säkerhet handlar om hur nationens befintliga, förändrade och nytillkommande resurser skall utnyttjas samordnat för att säkerställa tilliten till hantering av information. Motivet för IT-säkerhetsstrategin är att underlätta att skapa ett säkert informationssamhälle för alla.

IT-säkerhetsstrategin utgör en grund för informationssäkerhet och säkerhet i total betydelse. IT-säkerhetsstrategin utgör också en av utgångspunkterna för en nationell strategi för skydd mot informationsoperationer. Lika nödvändigt som det är att i fred bygga upp ett militärt försvar är att i fred förbereda skydd av samhället mot informationsoperationer. Därför måste den grundläggande IT-säkerheten utformas så att en smidig omställning av samhället kan ske för att snabbt skydda mot allvarliga informationsattacker.

Samhällets IT-säkerhet har stor betydelse för alla politikområden. Ingen säkerhet är hundra procentig, men de risker man tar skall vara medvetna och kvarvarande brister skall vara kända och motiverade.

Övergripande IT-politiska mål är att utveckla Sverige som en ledande IT- och Internetnation och att Sverige blir ett informationssamhälle för alla. Därför prioriteras tilliten till IT, kompetensen att använda IT samt tillgängligheten till informationssamhällets tjänster. För detta krävs att Sverige agerar föredömligt på IT-säkerhetsområdet.

7.2.2 Ansvar för IT-säkerhet

Varje enskild myndighet, organisation eller företag svarar för att den egna informationsbehandlingen sker med betryggande säkerhet. Detta medför att varje organisation i den offentliga förvaltningen och i näringslivet på en övergripande nivå skall kunna identifiera, bedöma och hantera sitt beroende av IT och de risker som finns förknippade med användningen av IT.

IT-säkerhet är till sin natur tvärsektoriell. För att åstadkomma ett helhetsperspektiv och en avvägd säkerhet mellan olika samhällsområden krävs en tvärsektoriell samordning genom samverkan och

samråd kännetecknad av förtroende, kompetens och bästa resursutnyttjande.

Riksdag och regering har ett övergripande helhetsansvar för samhällets informationsförsörjning och därmed även för informationssäkerhet främst när det gäller samhällsviktiga funktioner. Detta ansvar gäller lagstiftning och andra regelverk, den offentliga verksamhetens struktur, samordningsorgan och stödfunktioner för att skapa ett helhetsperspektiv. Ansvaret innebär också att staten skall främja uppbyggnaden av en grundläggande förmåga hos såväl samhällets myndigheter som kommunal förvaltning och näringsliv att hantera IT-säkerhet. Detta fräntar dock aldrig de enskilda organisationerna ansvaret för sin egen IT-säkerhet.

7.2.3 Säker teknisk infrastruktur

Samhällsviktiga funktioner inom alla samhällssektorer skall så långt möjligt skyddas från störningar och fungera störningsfritt såväl i fred som under svåra påfrestningar i samhället och i krig. Varje avbrott eller manipulation av dessa kritiska funktioner måste vara begränsat, sällan förekommande, hanterbart, isolerat och i så liten utsträckning som möjligt skadligt för nationens väl.

Risker måste kunna hanteras. Alternativa möjligheter har avgörande betydelse för att minska sårbarheten. För att kunna hantera frågor om infrastrukturens sårbarhet behöver viktiga system och nätverk identifieras och värderas. Kontinuerliga sårbarhetsanalyser och samlade bedömningar skall leda fram till prioriterade åtgärdsförslag, genomförande och uppföljning.

En mycket viktig del i samhällets IT-säkerhet är en säker infrastruktur för Internet. Sverige skall kunna bibehålla funktionaliteten och användbarheten hos Internet oberoende av funktioner och system som är placerade utanför landet eller som av andra skäl är utanför svensk kontroll. Med detta avses att Internet skall kunna användas för i huvudsak normal kommunikation mellan privatpersoner, offentlig verksamhet, företag och organisationer.

7.2.4 Grundläggande krav för IT-säkerhet

Krav på IT-säkerhetsåtgärder

All offentlig förvaltning skall bedrivas med betryggande säkerhet i internt arbete, arbete mellan myndigheter, arbete gentemot med-

borgarna och internationellt. Förvaltningen skall erbjuda en hög servicegrad och kunna nås elektroniskt samt kunna erbjuda tjänster för spridning och hämtning av information via allmänna kommunikationsmetoder. Detta skall ske med god tillförlitlighet, tillgänglighet och säkerhet. Det skall gå att säkert kommunicera inom landet och med omvärlden. Elektroniska affärer skall kunna bedrivas säkert. Ett informations samhälle för alla förutsätter även att hela den infrastruktur som informationen beror av är säker och har hög tillgänglighet. Krav ställs på förebyggande säkerhetsåtgärder, på säkerhetsåtgärder vid upptäckt av intrång och på reaktiva åtgärder. Säkerhetsåtgärder skall medge upptäckt vid försök till intrång samtidigt som de skall ge tillräckligt med tid för att hindra eller begränsa intrånget.

Tilltron till ny informationsteknik är i mycket stor grad beroende av tilltron till de tekniska systemens säkerhet. Det inkluderar tilltro till att systemen bevarar och garanterar sekretess, äkthet och riktighet avseende den information som hanteras. I förvaltnings-sammanhang är detta viktigt, inte minst för den personliga integriteten och medborgarnas trygghet.

Informationssäkerhet kräver helhetsperspektiv. Informationssäkerhet skall vara tvärsektoriell.

I informationsåldern omvandlas samhället från sektorer till nätverk. Detta kräver ett helhetsperspektiv på samhället. Säkerhetsarbetet blir gränslöst när gränserna mellan olika system suddas ut. Nätet har inte ett finare skydd än sin största maska, varför det behövs en gemensam grundläggande säkerhetsnivå i nätverkssamhället.

Enskild och offentlig verksamhet måste tillsammans sträva efter att höja denna säkerhetsnivå för att motstå verkan av samordnade angrepp på flera viktiga delar av samhället samtidigt. Informationssäkerheten skall hanteras tvärsektoriellt eftersom angreppen till sin karaktär kan vara samlade och samordnade. Nätet måste också vara tillräckligt starkt i varje viktig del för att allvarliga spridnings-effekter skall undvikas.

Säkerhetsmedvetenhet skall prägla all utveckling och förändring inom IT-området.

En god säkerhetsmedvetenhet är av grundläggande betydelse för informationssamhället. Säkerhetsfrågorna måste beaktas redan från första början vid all utveckling inom IT-området. Säkerhetsfunktioner som måste tillföras i efterhand innebär problem och ökade kostnader.

Säkerhetskrav grundas på fyra pelare: människor, regler, teknik och organisation.

En god helhetssyn förutsätter att säkerheten för vardera människor, regler, teknik och organisation är god och att säkerhetsnivåerna är harmoniserade och avvägda mot varandra. Det hjälper inte att exempelvis den tekniska säkerheten är hög om något av de tre andra områdena är förbisett i väsentligt avseende. Människors säkerhetsmedvetenhet och kompetens har stor betydelse. Regler och organisation är också grundläggande.

7.2.5 Strategiska uppgifter

Tväarsektoriell samordning på nationell nivå

Det övergripande arbetet med IT-säkerhet kräver en samordning som också är nödvändig för att skapa ett skydd mot informationsoperationer. Angrepp mot svenska IT-system kan vara samordnade och samtidigt slå mot flera sektorer i samhället. Osäkerheten om var och hur hot och störningar kan uppstå ökar behovet av en samordnande instans med överblick och kunskap om hur incidenter och konsekvenser skall hanteras och som kan vidta förebyggande åtgärder. P.g.a. den hastighet och de spridningseffekter IT-angrepp kan uppvisa, måste den nationella samordningen ha gemensam överblick och förmåga att med stor snabbhet hantera dynamiska skeenden.

Ett tväarsektoriellt samordningsorgan skall ansvara för sektorsövergripande frågor såsom behovsanalys och avvägningar mellan sektorer varunder viktiga verksamheter inom samhällets informationsinfrastruktur sorterar. Organet skall därför utgöra ett viktigt stöd till bl.a. Regeringskansliet för snabbt införande av de förslag och åtgärder som befinner sig på kallelistan. Organet kan i vissa lägen även

vara operativt. Alla delar av samhället behöver kunna representeras på hög nivå för en bred samverkan mellan privat och offentlig sektor.

Syftet med den tvärsektoriella samordningen och rådgivningen är

att bedöma sårbarhet och hotbild och förändringar av hotbilden med underlag från incidentanalys och övergripande omvärldsanalys

att föreslå hur sårbarheten och hotbilden kan omsättas i planeringstermer och optimal resursfördelning för skydd av berörda samhällssektorer

att föreslå åtgärder som kan omsättas i förebyggande verksamhetsstöd i form av råd och rekommendationer om IT-säkerhet

att åstadkomma en bred helhetssyn i förebyggande syfte, vid kriser och svåra IT-störningar och vara rådgivande till Regeringskansliet

att utgöra en krishanteringsresurs vid svåra IT-störningar i samhället.

IT-incidenthantering

Syftet med ett centralt stöd för IT-incidenthantering är att i realtid eller nära realtid tillse att attacker mot datasystem avstysas och upphör, samt stödja återställande av systemen vid större attackföretag. Incidentstödet skall ha översikt och kunskaper om IT-hot och IT-säkerhet i ett helhetsperspektiv. Förmåga krävs att kunna skilja okvalificerade och osystematiska intrångsförsök från kvalificerade och systematiska angrepp. Säkerhetsproblem som oklara fel, större avvikelser, incidenter och återstart av system som inte klaras ut av enskilda systemägare skall kunna hanteras. Kvalificerad rådgivning från en hjälpcentral skall kunna lämnas. Ansvaret kvarstår dock ytterst alltid hos systemägaren.

Samhällsviktiga funktioner skall ha tillgång till centralt stöd för IT-incidenthantering. Både enskild och offentlig verksamhet omfattas, eftersom viktiga delar av samhällets infrastruktur drivs i privat regi. Nationellt samarbete är väsentligt eftersom många funktioner är sammankopplade. Varning och larm måste kunna ske så tidigt som möjligt. Internationellt samarbete med utländska motsvarigheter bidrar till snabbare uppbyggnad av kompetensen inom IT-incidenthantering. För att representera Sverige internationellt behöver funktionen ges offentlig status.

Bearbetning av statistik över IT-incidenter skall medverka till kartläggning av bl.a. typer av intrång och deras inverkan på sårbarhet och betydelse för säkerheten. Detta kräver att en statistikfunktion gör en samordnad insamling, uppföljning och utvärdering av vad som framkommit vid de statliga myndigheternas IT-säkerhetsarbete. Statistikfunktionen skall vara en integrerad del i funktionen för IT-incidenthantering. Till en sådan statistikfunktion skall statliga verksamheter åläggas att rapportera alla definierade IT-incidenter. Incidentrapporter skall efter den centrala bearbetningen återremitteras till systemägaren för att kunna utgöra underlag för skyddsåtgärder.

Kommuner, landsting och privata företag bör genom avtal kunna ansluta sig till den centrala funktionen. En förutsättning att så sker är att den centrala funktionen bygger upp ett grundmurat förtroende som leder till att partnerskap kan etableras mellan de offentliga och privata sektorerna. Information måste kunna lämnas utan att svagheter blottställs som missgynnar förtroende och affärsverksamhet.

Incidentanalys

Incidentanalyserna baseras på uppgifter från det akuta incidentstödet, från statistik över incidenter och från samverkan med internationella organisationer som producerar varningar. Analyserna utgörs av djupgående tekniska undersökningar. Hot och risker skall kunna identifieras beträffande datorutrustning, program och nätverkssystem.

Varningar skall kunna utfärdas till bl.a. de trafikförmedlande operatörerna i händelse av överhängande hot. Den samordnade värderingen av tillgänglig information skall kunna resultera i såväl prognoser som strategiska varningar. I de delar näringslivet medverkar är det helt avgörande att känslig information om företags-specifika förhållanden inte sprids.

Övergripande omvärldsanalys

Förändringar av hot och sårbarheter på IT-området måste kunna följas nationellt och internationellt med hjälp av strategiska och taktiska omvärldsanalyser som får stöd av civila och militära under rättelse- och säkerhetsfunktioner. Omvärldsanalysen med sikte på

IT-säkerhet har även anledning att ur ett helhetsperspektiv uppmärksamma besläktad utveckling inom IT-relaterade medier som kan rubriceras som desinformation, psykologiska operationer eller andra former av informationsoperationer i dess vidaste bemärkelse.

Omvärldsanalyserna skall sammansättas med incidentanalyser för att utröna aktörer, metodik och motiv för intrång. Hotbilder skall sammansätta med IT-sårbarhet i samhället möjliggöra bedömning av sannolikhet och risk för angrepp och konsekvenser härav.

Hotbilder skall identifieras som anger

tänkbara angripares identiteter och avsikter
tänkbara tekniker, metoder och förmågor för angrepp
tänkbara mål, allt ifrån nationell till individuell nivå.

Aktiv IT-kontroll

Aktiv IT-kontroll syftar till att genom verkliga intrångstester påvisa säkerhetsbrister och svaga punkter i de aktuella IT-systemen. Efter att svaga punkter identifierats är det av stor vikt att dessa analyseras och ligger till grund för konkreta förslag på skyddsåtgärder. Detta är viktiga led för att förbättra IT-säkerheten, inte minst genom den uppmärksamhet som normalt uppkommer hos systemförvaltare vid aktiv IT-kontroll. Uppmärksamheten höjer medvetenheten och intresset, vilket i sig är säkerhetsbefrämjande.

Aktiv IT-kontroll skall utövas i en funktion med hög teknisk kompetens, som skall kunna vara en resurs inom hela statsförvaltningen men även kunna stödja samhället i övrigt enligt en övergripande inriktning.

Förebyggande verksamhetsstöd

I förebyggande syfte skall sammanhållna råd och rekommendationer inom IT-säkerhetsområdet snabbt kunna göras tillgängliga för enskild och offentlig verksamhet och utgöra stöd för det distribuerade ansvaret bland samhällets IT-användare. Det skall medverka till att göra den offentliga förvaltningen till en effektiv och säker användare och föregångare på IT-området med bibehållna krav på insyn, på sekretess och säkerhet samt på skydd av enskildas personliga integritet.

Kunskap inom IT-säkerhet ställer krav på program för utbildning och ständig vidareutveckling. Det är av stor vikt att ledning-

arna inom såväl enskild som offentlig verksamhet tar ett särskilt ansvar för att deras anställda ges lämplig utbildning i IT-säkerhet.

Alla som är förvaltningsansvariga för system eller information av samhällsviktigt slag skall göra regelbundna risk- och säkerhetsanalyser med upprättande av handlingsplaner för ett kontinuerligt säkerhetsarbete. Dessa planer skall utgöra en del av revisionen. Därigenom blir frågorna samtidigt ledningsfrågor för exekutiv ledning och styrelse utan att något omfattande regelverk behöver tillskapas. Erfarenhet och metodik att upprätta handlingsplaner kan utnyttjas från arbetet med att förbereda system inför skiftet till år 2000.

Samhället i allmänhet och totalförsvaret i synnerhet behöver ha en uppfattning om vilken säkerhetsnivå olika IT-produkter har. Därför behövs ett system för evaluering och certifiering av sådana produkter.

Forskning, utveckling och högskoleutbildning

IT-säkerhetskunskap skall hålla hög kvalitet och vara aktuell i det snabbt föränderliga informationssamhället. En grundläggande förutsättning för att nationen skall bli ledande på IT-säkerhet är att universitet och högskolor intar en ledande ställning inom forskning, utveckling och utbildning. Kombination av teoretiska kunskaper med aktuella praktiska erfarenheter och förmåga att utnyttja teori och praktik har en avgörande betydelse. Detta kräver också att universitet och högskolor får ett nära och fruktbara samarbete med näringslivet och med de delar av den offentliga verksamheten som har dagliga uppgifter inom området. Det gäller inte minst grupper som upptäcker incidenter och grupper som genomför omvärlds- och incidentanalys med anknytning till IT.

Lagar och regler

Den snabba utvecklingen på IT-området kräver att lagstiftning och andra regelverk utvecklas tillräckligt snabbt. Det bör eftersträvas att skapa ett harmoniserat och sammanhållet regelverk för informationssäkerhet som möjliggör överblick och entydig tillämpning.

Internationellt arbete

Informationssamhället är gränslöst och kräver internationellt samordnade och samverkande organ för att motverka skilda angrepp. Tydliga riktlinjer skall tas fram som kan styra den svenska hållningen i strategiskt viktiga frågor avseende det internationella säkerhetsarbetet. Sverige skall aktivt stödja internationella avtal och regler för att främja informationssäkerhet. Sverige skall, grundat på våra principer för specifika intressen, aktivt medverka i sammanhang där frågor om gemensamma standarder och normer för säkerhet, informationsförsörjning och IT-infrastruktur behandlas.

Sverige skall aktivt stödja internationella avtal och regler för spårning av obehörig verksamhet inom data- och informationsområdet. Sådan spårning kan behöva ske över nationsgränser utan tidsfördröjning. Rättssäkerhet och integritet skall beaktas.

Sverige skall aktivt stödja internationella avtal och regler för att öka skyddet mot informationsoperationer som kan skada demokratiska värden. Informationssäkerhet har stor betydelse för hantering av informationsoperationer. Frågorna har en plats inom Europeiska unionen och Europarådet. Det är också viktigt att på global nivå kunna skapa en gemensam principiell grund för skydd mot informationsoperationer som kan skada demokratiska värden.

7.3 Samordningsorgan för IT-säkerhet

IT-säkerhetsfrågorna har stor betydelse för samhället och är tvärsäkerhetsfrågor till sin natur. Inom Regeringskansliet berörs flera departement av dessa frågor. Detta gäller bl.a. Försvars-, Justitie-, Närings- och Utrikesdepartementen. Så gott som samtliga departement berörs dock indirekt såtillvida att den verksamhet som de är ansvariga för i samhället i större och mindre omfattning är IT-beroende och därför måste säkras mot olika typer av IT-hot.

På myndighetsnivå föreslås planeringsmyndigheten få ett övergripande ansvar för IT-säkerhetsfrågorna. I denna uppgift ligger ett ansvar för samordningen av de åtgärder som vidtas på myndighetsnivå för att avvärja IT-hot. Enligt utredningens uppfattning bör en motsvarande samordningsfunktion finnas inom Regeringskansliet. Denna bör ha ett särskilt ansvar för frågor som gäller skydd mot informationsoperationer. Utredningen föreslår därför att ett sam-

ordningsorgan för IT-säkerhetsfrågor inrättas inom Regeringskansliet.

Samordningsorganet bör även ha uppgifter i akuta situationer vid allvarliga händelser som hotar IT-säkerheten. Uppgiften bör då vara att följa utvecklingen med utgångspunkt från underlag som tas fram av planeringsmyndigheten och andra organ. Samordningsorganets uppgift i sådana situationer bör också vara att ta fram underlag för brådskande regeringsbeslut om sådana krävs i den situation som har uppstått. I mycket allvarliga situationer bör samordningsorganet samverka med det nationella krishanteringsorgan som utredningen föreslog i kapitel 5. Ett sådant behov torde främst uppstå om hotet utgörs av informationsoperationer som har stor omfattning eller riktar sig mot särskilt känsliga funktioner i samhället. Detta bör också gälla för allvarliga kriser som har ett väsentligt inslag av IT-relaterade hot.

Samordningsorganet för IT-säkerhet bör bestå av företrädare för olika departement och myndigheter. Företrädare för andra sektorer, t.ex. näringslivet, bör också ingå i organet. Organet bör vara en del av Regeringskansliet. I likhet med det nationella krishanteringsorganet bör samordningsorganet inte ha några formella beslutsbefogenheter. Beslut bör normalt tas av berörda myndigheter och andra organ i enlighet med ansvarsprincipen. Samordningsorganet har också möjlighet att föreslå att regeringen fattar beslut i vissa frågor. Planeringsmyndigheten bör fungera som kansli åt samordningsorganet. Starka skäl motiverar att planeringsmyndigheten i egenskap av IT-säkerhetsmyndighet har denna uppgift.

7.4 Funktionen för teknikkompetens inom IT-säkerhet

7.4.1 Allmänt

Samhället har behov av teknisk expertis för en mängd olika IT-säkerhetsfrågor. Det finns ett övergripande samhällsbehov av utveckling, analysförmåga och teknisk rådgivning inom IT-säkerhet. Det finns också hos enskilda myndigheter och företag ett behov av teknisk kompetens inom IT-säkerhet. Den privata konsultmarknaden har i dag ett brett utbud av tjänster av hög kvalitet på IT-säkerhetsområdet. Myndigheter och företag med behov av tillskott av kompetens på området har all anledning att utnyttja denna resurs.

Behovet av ökade satsningar på IT-säkerhet understryks av det faktum att flertalet IT-produkter traditionellt inte har utvecklats med beaktande av säkerhet. Tidigare var säkerheten ett marginellt problem. Kostnad och funktionalitet var de två enda parametrarna av väsentligt intresse. I dag är situationen annorlunda när datorerna har kopplats samman i nätverk, med Internet som det riktigt stora globala nätverket. Verkningsfull säkerhet kräver att säkerhetsaspekterna vägs in från början i all utveckling. Men även i dag förekommer det att IT-produkter utvecklas med bristfällig säkerhet. Det finns också ett stort antal gamla produkter i omlopp. Människan får inte heller glömmas bort i sammanhanget. Även om säkerheten i princip finns och är god i en produkt, kan den kräva en aktiv medverkan av användaren för att kunna utnyttjas. Därför återstår ännu många steg innan alla IT-produkter har en god säkerhet som är lätt att utnyttja och som inte är ett allvarligt hinder för funktionaliteten.

7.4.2 Motiv för ett statligt engagemang

Det finns enligt utredningens uppfattning starka skäl som talar för att staten skall kunna erbjuda en hög teknisk kompetens och ett avancerat tekniskt stöd i IT-säkerhetsfrågor:

Förtroende

Försvars- och säkerhetspolitiskt behov av skydd för känsliga uppgifter

Garanterad resurs mot informationsoperationer eller andra säkerhetskritiska situationer

Officiell samverkan i internationella sammanhang

Förtroende

De flesta organisationer har hög sekretess kring sina IT-säkerhetsförhållanden. En del organisationer tvekar inför att ge enskilda aktörer det förtroende som krävs för att lösa känsliga säkerhetsproblem (liksom det även finns exempel på organisationer som tvekar att ge staten ett sådant förtroende). Organisationen tvingas ta riskerna med att exponera sina allra känsligaste informations säkerhetsproblem. Detta problem blir särskilt tydligt för de organisationer som själva saknar kompetens på området. Dessa saknar normalt möjlighet att själva bedöma hur seriösa och kompetenta enskilda aktörer är.

Försvars- och säkerhetspolitiskt behov av skydd för känsliga uppgifter

Problemet med förtroende uppkommer också när det gäller säkerhetskritisk teknik för totalförsvaret eller andra kunder i samhället med försvars- eller säkerhetspolitiskt känslig verksamhet. Dessa kunder kan inte i alla lägen förlita sig helt till utbudet av varor och tjänster på marknaden, utan behöver tillgång till teknisk kompetens inom staten för att med en god beställarkompetens så långt det överhuvudtaget är möjligt skydda sig mot avsiktliga eller oavsiktliga säkerhetsbrister. Att utföra uppgifter av betydelse för rikets säkerhet kan inte enbart lämnas till enskilda aktörer på marknaden.

Garanterad resurs mot informationsoperationer eller andra säkerhetskritiska situationer

Staten behöver säkerställa tillgång till en viss teknisk kompetens att användas bl.a. i säkerhetskritiska situationer. Skulle Sverige t.ex. plötsligt vara utsatt för en informationsoperationsattack kan det vara förödande om det inte finns någon instans med teknisk expertis garanterat tillgänglig.

Staten har ett ansvar att hantera skyddet mot informationsoperationer. IT-säkerhet är en viktig komponent i detta skydd, varför staten måste ha en teknisk kompetens på detta område, att användas i förebyggande arbete, vid nationella kriser med IT-inslag eller till att snabbt ta fram skydd mot elakartade program.

Officiell samverkan i internationella sammanhang

Datakommunikation är i sig en internationell och gränslös företeelse. Därav följer att IT-säkerhet i högsta grad är en internationell fråga. Sverige måste delta i de internationella nätverk som finns och bildas på området. Därför behöver också staten ha en resurs med hög teknisk kompetens för att kunna delta i dessa nätverk och aktivt kunna tillföra kunskaper i arbetet.

Det finns sålunda skäl att inrätta en statlig eller statligt understödd funktion med hög teknisk kompetens inom IT-säkerhet. Detta får dock inte innebära att staten skall bedriva någon konkurrens på konsultmarknaden.

7.4.3 Uppdragsgivare

Teknikkompetensfunktionen bör arbeta kundorienterat. Uppdragen som utförs skall alltid vara beställda direkt av kunden och inte av funktionen själv eller av en tredje part.

I princip hela samhället skall kunna vara kunder till funktionen. Den viktigaste målgruppen är dock statliga myndigheter, främst totalförsvarsmyndigheter och myndigheter med särskilda säkerhetsbehov. Kommuner och landsting samt privata företag och organisationer som utgör väsentliga samhällsintressen kan vara en annan målgrupp. Funktionen kommer dock att ha begränsade resurser och blir därför tvungen att starkt prioritera sina uppdrag.

Om andra företag, organisationer eller enskilda personer vill anlita teknikkompetensfunktionen bör funktionen efter avtal kunna hjälpa dessa så länge det inte går ut över mer prioriterade uppgifter. Kundkretsen kan dock inskränkas något i och med att tekniska säkerhetslösningar kan användas för att dölja brottslig verksamhet. Teknikkompetensfunktionen måste säkerställa att den inte understöder oseriös verksamhet, bidrar till oegentligheter eller skapar grund för brottslighet.

För att kunna fullgöra uppgiften att vara en resurs av hög kvalitet för samhället i teknisk IT-säkerhet, krävs att teknikkompetensfunktionen kontinuerligt inhämtar kunskaper och information samt upprätthåller kontakter såväl nationellt som internationellt.

Funktionen måste hela tiden besitta mycket hög teknisk kompetens. Kunskaper måste finnas både på ett allmänt plan om tekniska principer för IT-säkerhet och mer specifikt om produkter på marknaden, i synnerhet om dem som används i större omfattning av offentliga sektorn, framför allt totalförsvaret. De tekniska detaljkunskaperna om produkter, protokoll, kända tekniska säkerhetsbrister och virus m.m. måste vara sökbara i informationsdatabaser.

7.4.4 Samverkan med andra organ

Samarbete måste utvecklas med andra organisationer på IT-säkerhetsområdet både inom och utom landet. Inom Sverige bör alla se IT-säkerhet som ett mål av gemensamt samhällsligt intresse där samarbete är en viktig faktor för att lyckas. IT-säkerhet är dessutom en gränslös fråga där problemen oftast är likartade världen

över, vilket motiverar ett långtgående internationellt samarbete. Detta kan exempelvis gälla utbyte av metodik och erfarenheter, samarbete om analys av elakartade program eller överenskommelser om evalueringskriterier. Skulle dessutom en allvarlig kris med IT-inslag inträffa är den sannolikt inte geografiskt begränsad till Sverige. Då blir ett internationellt samarbete helt nödvändigt. Kontakter skall därmed hållas med IT-säkerhetsorganisationer i andra länder, såsom t.ex. BSI¹¹ i Tyskland och CESG¹² i Storbritannien.

Funktionen bör vara drivande i arbetet att bilda internationella nätverk, främst globala men även på europeisk nivå, bl.a. med syfte att harmonisera tekniska IT-säkerhetslösningar och att ha en beredskap inför internationella kriser med IT-inslag.

Det krävs också kontakter med IT-leverantörer, t.ex. för att effektivt kunna utföra evalueringar, för att kunna påverka säkerhetslösningar eller för att kunna identifiera potentiella tekniska sårbarheter som kan uppkomma antingen direkt i produkterna eller i kombination med någon annan produkt eller inom något slags system.

7.4.5 Teknikkompetensfunktionens uppgifter

Teknikkompetensfunktionen bör kunna verka inom nedanstående områden. Utredningen vill dock betona att verksamheten bör ha begränsad omfattning, vilket medför att uppdragen måste prioriteras hårt. Teknikkompetensfunktionen bör inte heller uppträda som aktör på konkurrensutsatta marknader.

- Evaluering av IT-produkter

- Medverkan i utveckling av IT-säkerhetsprodukter och säkerhet i IT-produkter

- Utbildning, information och rådgivning om teknik inom IT-säkerhetsområdet

- Insatser mot informationsoperationer eller vid nationella kriser med IT-inslag

- Aktiv hjälp vid svåra IT-säkerhetsincidenter

- Aktiv IT-kontroll

- Analys av elakartade program

- Annat tekniskt stöd inom IT-säkerhetsområdet

¹¹ BSI = Bundesamt für Sicherheit in der Informationstechnik

¹² CESC = Communications-Electronics Security Group

Evaluering av IT-produkter

Samhället i allmänhet och totalförsvaret i synnerhet behöver tilltro till att de säkerhetsfunktioner som finns i olika IT-system verkligen utgör det skydd man förväntar sig. Detta gäller för såväl egenutvecklade produkter som kommersiella produkter. En sådan tilltro kan skapas med ett system för att evaluera och certifiera IT-produkter och IT-system. Med evaluering avses här en formell säkerhetsgranskning av en produkt eller ett system i syfte att skapa en tilltro till att säkerhetsfunktionerna i produkten eller systemet har en adekvat skyddsförmåga. Med certifiering avses här ett utfärdande av certifikat, dvs. ett fastställande av resultat av evaluering och ett bevis att denna gjorts enligt fastställd metodik och med rätt kompetens. Målet med en evaluering är att erhålla ett certifikat. Certifikatet ger användaren en tilltro till produktens säkerhet. Beställaren av en evaluering är normalt en produktutvecklare, men kan för speciella produkter ibland vara kunden. För en säljare ger ett certifikat ett mervärde till produkten och kan vara ett viktigt försäljningsargument. För en kund ger ett certifikat ett bevis på att produkten på en given granskningsnivå uppfyller de säkerhetskrav man har ställt.

Sverige har i dag, till skillnad från många andra tekniskt utvecklade länder, inget system för evaluering och certifiering. För tilltron till säkerhetsfunktionerna i IT-system bör Sverige följa omvärldens exempel och inrätta ett system för evaluering och certifiering. Det är viktigt att hålla isär dessa båda moment. Evaluering är en teknisk granskningsprocess, medan certifiering är en process som syftar till att säkerställa kvalitet och objektivitet i den utförda evalueringen. Det finns alltid en risk att evalueringen blir bristfälligt utförd om samma instans också gör certifieringen, genom att instansen därmed får lättare att tillfredsställa kundens dvs. systemkonstruktörens vilja att erhålla ett certifikat. I andra länder görs normalt evalueringen av särskilt godkända evalueringsföretag, utom i fråga om försvars- eller säkerhetspolitiskt särskilt känsliga system, medan certifieringen görs av respektive lands IT-säkerhetsmyndighet. Som exempel kan nämnas att i Tyskland gör myndigheten BSI¹³ certifieringar. Certifiering och evaluering diskuteras mer ingående i avsnitt 7.7.

I och med att Sverige f.n. saknar ett system för evaluering och certifiering har inga evalueringsföretag etablerat sig. Innan sådana hinner etablera sig kan teknikkompetensfunktionen utföra evaluate-

¹³ BSI = Bundesamt für Sicherheit in der Informationstechnik

ringar. Men även efter det att evalueringsföretag etablerat sig bör funktionen ha möjlighet att evaluera vissa typer av IT-produkter. Staten behöver upprätthålla kompetensen, samtidigt som vissa kunder, t.ex. totalförsvaret, har så höga sekretesskrav att de inte alltid kan vända sig till den privata marknaden för evalueringar.

IT-system kan innehålla kryptografiska delar. Kryptografi är en viktig metod för att erhålla sekretess. Genom att data krypteras är avsikten att en obehörig som på ett eller annat vis fått tillgång till krypterad data inte skall kunna ta del av informationsinnehållet. Sekretessbelagd information som skall kommuniceras över en kanal som inte är garanterat skyddad för avlyssning, t.ex. Internet, måste vara krypterad. Även sekretessbelagd information som endast ligger lagrad på t.ex. en hårddisk utan att kommuniceras kan behöva krypteras om det finns risk att någon obehörig kommer åt hårddisken, kanske genom stöld. Kryptografiska metoder kan även användas för att skapa elektroniska signaturer. Rätt använda utgör dessa en garanti för riktighet och autenticitet, dvs. att informationen inte har förändrats och att informationen har rätt avsändare.

Varje krypto bygger på en eller flera algoritmer, dvs. en följd av matematiska beräkningssteg för att omvandla klartext till kryptotext och vice versa. Det finns outsinliga möjligheter att skapa kryptografiska algoritmer¹⁴ för att erhålla sekretess, autenticitet och riktighet. Inom totalförsvaret används oftast eget utvecklade, hemliga algoritmer. Kvaliteten på kryptoalgoritmer kan variera avsevärt. En alltför svag algoritm gör att någon obehörig kan forcera det skydd man har skapat. Ju svagare algoritm desto mindre beräkningskapacitet behöver en obehörig för att forcera den.

Evalueringar omfattar normalt sett inte att utföra kryptologiska bedömningar av de ingående algoritmernas styrka. Dessa bedömningar har i dag Totalförsvarets signalsskyddssamordning (TSA)¹⁵ ensamrätt på inom totalförsvaret, och bör alltså ha så av kompetensskäl. För vissa IT-system med höga krav på sekretess, autenticitet eller riktighet kan det dock vara motiverat att utföra kryptologiska bedömningar i samband med evaluering. Behovet av detta har kraftigt ökat de senaste tio åren med integreringen av ADB-system och kommunikationssystem. Av detta följer att även teknikkompetensfunktionen måste ha ett nära samarbete med TSA. TSA har f.ö. en nära koppling till och intimt samarbete i metodik- och kompetensfrågor med Försvarets radioanstalt (FRA), som är den svenska signalspaningsorganisationen med

¹⁴ Vanliga öppet kända algoritmer är t.ex. DES, RSA och MD5

¹⁵ TSA organiseras f.n. av FM/MUST

ansvar att utföra kryptologisk analys på den spanade radiotrafiken. Denna koppling är mycket värdefull då den starkt bidrar till ett gott svenskt signalskydd. TSA kan därmed undvika de slags misstag som FRA söker utnyttja i sin analys av utländsk krypterad kommunikation.

Medverkan i utveckling av IT-säkerhetsprodukter och säkerhet i IT-produkter

IT-säkerhetsprodukter är sådana vars huvudsyfte är att stärka IT-säkerheten. Det kan gälla brandväggar, antivirusprogram, krypteringsutrustning, m.m. Säkra IT-produkter är sådana som i huvudsak har en annan funktionalitet än IT-säkerhet, men som är konstruerade med beaktande av IT-säkerhetskrav. Båda slagen av produkter är viktiga för att ge en god IT-säkerhet. Säkra IT-produkter krävs för att inte sårbarheter skall uppkomma vid användande av IT-system. IT-säkerhetsprodukter krävs för att medverka till att skapa ett skydd mot olika hot mot IT-system.

Dessa typer av produkter behöver ständigt utvecklas. Dessutom finns det kunder som har särskilda behov och inte kan nöja sig med de standardprodukter som finns på marknaden. För dessa kunder kan en statlig teknikkompetensfunktion ge ett värdefullt stöd med att bevaka de säkerhetsaspekter som finns.

En statlig teknikkompetensfunktion skall inte i första hand själv bedriva utveckling av sådana produkter annat än möjligen för laborationsändamål eller för att ta fram något mycket enkelt program. Däremot skall funktionen kunna utgöra en resurs för att bl.a. inför upphandlingar se till att kravspecifikationer uttrycker den säkerhetsnivå som en kund bör kräva. I vissa fall kan funktionen även utföra tester och verifiera att kraven uppfyllts.

Det militära försvaret är en kund som har behov av icke-kommersiella IT-produkter. Därmed skulle Försvarsmakten i princip kunna vara en kund till teknikkompetensfunktionen för att få stöd med säkerhetsaspekterna vid utveckling av IT-produkter. Det finns dock sannolikt starka skäl för Försvarsmakten att själv ha kompetensen att kunna definiera krav på IT-produkter, om än inte resurserna att i detalj utveckla dem. Stödet som teknikkompetensfunktionen kan erbjuda Försvarsmakten kan då i stället vara att oberoende kunna granska föreslagna lösningar.

Utbildning, information och rådgivning om teknik inom IT-säkerhetsområdet

Kunskapsförmedling inom IT-säkerhet är generellt sett viktigt. En ökad medvetenhet och en höjd kunskapsnivå i samhället är kanske den enskilt viktigaste åtgärden för att stärka samhällets IT-säkerhet. Teknikkompetensfunktionen bör delta i kunskapsförmedlingen på det tekniska området.

Utredningen föreslår att det vid sidan av teknikkompetensfunktionen inrättas en IT-incidenthanteringsfunktion, som bl.a. föreslås få en informationsförmedlande roll i bred bemärkelse avseende IT-säkerhet. Arbetsuppdelningen dem emellan är lämpligen att teknikkompetensfunktionen arbetar direkt mot kund med information och råd som kräver en djupare teknisk kompetens, medan IT-incidenthanteringsfunktionen ger råd som är av allmängiltig natur till en kund samt sprider information på bred front till samhället i stort.

Teknikkompetensfunktionen bör kunna anordna seminarier, föreläsningar och även vissa kortare utbildningar inom smala tekniska spetsområden med anknytning till IT-säkerhet. Syftet är att komplettera marknaden inom viktiga specialområden som marknaden inte erbjuder utbildning i.

IT-incidenthanteringsfunktionen kan vara kund till teknikkompetensfunktionen i fråga om att ta fram information om teknisk IT-säkerhet till samhället. Det kan t.ex. gälla information om hur man installerar och underhåller brandväggar, viruskydd, logganalys, m.m. IT-incidenthanteringsfunktionen har sedan ansvaret för att sprida informationen vidare i lämplig form, t.ex. på webbsidor.

För att erhålla en hög säkerhet kan kunder behöva rådgivning inte enbart om teknik, utan även om organisation, regler och människa. Man kan därför överväga att för att erhålla en helhet även låta funktionen ha möjlighet att ge rådgivning om kompetens- och utbildningsbehov inom IT-säkerhet, organisationskrav eller regelverk. Andra möjligheter är att låta den föreslagna planeringsmyndigheten eller IT-incidenthanteringsfunktionen svara för denna rådgivning, då den inte är av utpräglad teknisk natur.

Utbildning som redan finns på marknaden skall däremot inte teknikkompetensfunktionen erbjuda. Det finns ingen anledning att konkurrera med den privata marknaden om att anordna utbildning. Det är inte heller meningen att funktionen skall erbjuda akademisk utbildning. Sådan utbildning erbjuds i dag av universitet och högskolor. I den mån den akademiska utbildningens kvantitet eller

kvalitet skulle bedömas otillräcklig inom IT-säkerhetsområdet är det en brist som måste åtgärdas inom ramen för högskolesystemet.

Insatser mot informationsoperationer eller vid nationella kriser med IT-inslag

Skulle Sverige bli utsatt för en informationsoperationsattack på bred front kan det krävas ett övergripande samarbete mellan flera instanser med kompetens inom IT för att attacken skall kunna avvärijas och för att genomföra eventuell restauration efter attacken. Ett motsvarande övergripande samarbete kan krävas vid andra typer av nationella kriser med IT-inslag. I sådana lägen utgör teknikkompetensfunktionen en viktig komponent i ett samlat, övergripande arbete med tekniska åtgärder. Funktionen bör då övergå till att sätta huvuddelen av sina resurser på att bemöta krisen.

Det finns anledning att diskutera befogenheter och ansvarsförhållanden vid informationsoperationsattacker eller vid nationella kriser med IT-inslag. Men det finns inga starka skäl som talar för att teknikkompetensfunktionen skall ha ett egentligt ledningsansvar ens i sådana lägen. Möjligen kan den undantagsvis få ett delegerat ansvar att leda de tekniska insatserna om särskilda omständigheter talar för detta.

Vid informationsattacker och nationella kriser med IT-inslag där problemen drabbar flera samhällssektorer, bör det tvärsektoriella samordningsorganet vara beställare av funktionens tjänster.

Aktiv hjälp vid svåra IT-säkerhetsincidenter

När en organisation drabbas av en IT-incident och rapporterar denna till en funktion för IT-incidenthantering kan organisationen samtidigt erhålla viss hjälp. Denna hjälp är inte alltid tillräcklig. Problemet kan vara generellt svårlöst eller omöjligt att lösa över telefon, eller också kan problemet vara av en så avancerad natur att det kräver hantering av särskild teknisk kompetens. Teknikkompetensfunktionen kan bistå med särskilt avancerad rådgivning, och kan även bistå med hjälp på plats.

I vissa fall vet inte den anmälade organisationen vad som är orsaken till incidenten. Teknikkompetensfunktionen kan bistå med felsökning. Arbetet kan vara tidskritiskt, t.ex. om ett samhällsvik-

tigt IT-system inte fungerar och man inte vet orsaken till detta. Dessutom är det viktigt att utröna om incidenten beror på brottslighet, t.ex. dataintrång. Eftersom den anmälade organisationen skall göra polisanmälan vid brottsmisstanke kan polisen komma att ställa krav på de åtgärder som vidtas. Teknikkompetensfunktionen skall ha sådan kännedom om polisiärt arbete att åtgärderna funktionen rekommenderar inte försvårar utan helst underlättar en senare polisutredning.

Man kan överväga om polisen skall kunna avropa tjänster från teknikkompetensfunktionen för att genomföra polisiärt arbete i en annan organisations miljö. Det kan gälla allt från spårning av brottslighet hos en drabbad organisation till tekniskt stöd vid husrannsakan. För detta talar att teknikkompetensfunktionen redan kan ha ett försprång i kunskapsnivå genom att en drabbad organisation redan anlitat funktionen när de upptäckte incidenten. Funktionen kan besitta viss spetskompetens som polisen saknar, eller också kan funktionen utgöra en möjlighet även för polisen att avropa vid toppar i belastningen. Mot detta talar förtroendet för funktionen. Organisationer kan komma att tvivla på att det är ett stöd de anlitat och inte en polisutredning. Behovet av förtroende gör att man inte bör låta teknikkompetensfunktionen delta aktivt i polisutredningar utan medgivande av den organisation hos vilken undersökningen skall ske.

Aktiv IT-kontroll

Ett av de effektivaste sätten att höja en organisations medvetenhet om behovet av IT-säkerhet är att utföra aktiv IT-kontroll. Genom att låta behöriga personer göra kartläggningar av nätverk, in-trångsförsök, m.m., upptäcks säkerhetsbrister, inte minst vad gäller konfiguration och användning, förhoppningsvis innan obehöriga personer upptäcker dem. En av de viktigaste effekter som därigenom uppnås är att man får en uppmärksamhet inom organisationen och därmed en ökad medvetenhet om IT-säkerhet.

Den som utför aktiv IT-kontroll skall inte ha något ansvar för att åtgärda de brister som upptäcks. Det är enbart den kontrollerade organisationens uppgift att avgöra på vilket sätt det skall ske.

Det är av nationellt strategiskt värde att aktiv IT-kontroll regelbundet genomförs på totalförsvarsmyndigheter och andra organisationer med samhällsviktiga IT-system. Teknikkompetensfunktionen bör kunna erbjuda denna tjänst till de organisationer som så

önskar på direkt uppdrag från dessa. Eftersom funktionen därigenom potentiellt kan få insyn i några av samhällets mest sekretessbelagda system är det oundgängligt att funktionen själv måste kunna garantera strängaste sekretess.

Man kan i och för sig överväga om teknikkompetensfunktionen även skall kunna agera på uppdrag av en tillsyns- eller revisionsmyndighet. För detta talar att tillsyns- och revisionsmyndigheter inte nödvändigtvis själva måste bygga upp den tekniska kompetensen. Mot detta talar att teknikkompetensfunktionen inte bör agera utan fullt förtroende från den organisation funktionen agerar hos. Behovet av förtroende för teknikkompetensfunktionen får anses väga tyngre än det eventuella behov av extern kompetens en tillsyns- eller revisionsmyndighet kan ha. Problemet kan alltid lösas genom att den kontrollerade organisationen ger sitt förtroende till teknikkompetensfunktionen att utföra aktiv IT-kontroll för en tillsyns- eller revisionsmyndighets räkning.

Det finns ett antal juridiska oklarheter kring aktiv IT-kontroll. Det är inte nödvändigtvis självklart att en statlig myndighet anses ha mandat att låta utföra aktiv IT-kontroll på sina system och nätverk. Systemen kan innehålla sekretessbelagd information, varför det är oklart om en myndighet kan anses ha följt de lagar och förordningar som gäller om sekretess när man låter en extern part utföra aktiv IT-kontroll. Aktiv IT-kontroll faller sannolikt inte under sekretesslagens 13 kap., som behandlar överföring av sekretess till annan myndighet. Vidare kan alltid störningar och skador inträffa p.g.a. själva kontrollen, även om den som utför den ålägger sig försiktighet. Ett annat problem är att man vid aktiv IT-kontroll oavsiktligt kan komma att hamna utanför de nätverk man skall kontrollera. Detta kan t.ex. bero på okända eller bortglömda förbindelser. Vad gäller om man kommer till en annan myndighet, kriminalregistret, ett privat företag, eller för den delen utanför landet? Dessa frågor bör utredas ytterligare så att eventuella författningsändringar skyndsamt kan genomföras för att göra aktiv IT-kontroll till ett hjälpmedel som kan användas med fullt legalt stöd.

Värt att notera är att brottsbalkens paragraf om dataintrång inte utesluter aktiv IT-kontroll. För att dataintrång skall anses föreligga måste denna vara olovlig. I och med att aktiv IT-kontroll alltid utförs på begäran av den som äger systemen torde den inte kunna anses vara olovlig i lagens mening.

Analys av elakartade program

Elakartade program kan vara t.ex. datavirus, maskar eller trojaner. Med jämna mellanrum drabbas samhället av elakartade program som kan ställa till stor skada på mycket kort tid, och därmed hota vitala samhällsfunktioner. Spridningen sker ofta via e-post. Tiden det tar för programvaran att sprida sig över stora delar av världen har kunnat röra sig om enbart timmar. Framtida teknik kan leda till att elakartade program sprider sig ännu snabbare.

Att larma och utfärda varningar är en uppgift för en IT-incidenthanteringsfunktion. Om ett larm eller en varning beror på att nyupptäckta elakartade program eller misstänkta sådana snabbt håller på att sprida sig i stil med Melissa 1999 eller Love letter 2000, bör dock även teknikkompetensfunktionen kopplas in för att ta fram tillfälliga skydd samt åtgärder för att sanera och återställa. Sannolikt räcker det ofta med att sammanställa, kanalisera och eventuellt göra en svensk anpassning av lösningar som kommer från olika kommersiella antivirusföretag, vars tjänster funktionen bör utnyttja i möjligaste mån. Men om så krävs skall teknikkompetensfunktionen själv kunna analysera elakartade program och ta fram de skydd och motåtgärder som krävs. Även om exemplen är få eller inga på elakartade program som är specifikt riktade att slå mot enbart svenska IT-system är det tekniskt möjligt att framställa sådana. Generella elakartade program kan också ha sitt ursprung i Sverige. I dessa fall är det möjligt att en svensk teknikkompetensfunktion har bättre förutsättningar än någon annan att snabbt ta fram skydd och motåtgärder.

För att kunna fullgöra uppgiften att analysera elakartade program måste teknikkompetensfunktionen ha spetskunskaper på området. För att skydda samhället mot besvärliga överraskningar i form av elakartade program som bygger på någon ny princip, bör funktionen i möjligaste mån ha kunskaper om principer för elakartade program redan innan dessa principer har använts i realiteten. Det kan därför övervägas om funktionen bör bedriva egen forskning och eget utvecklingsarbete i ämnet.

Sannolikt är det dock tillräckligt om teknikkompetensfunktionen har täta kontakter med forskare och organisationer som sysslar med denna forskning inom och utom landet. Inom de områden där behov av ny forskning finns kan funktionen initiera denna forskning hos någon institution. Lämpliga kontakter inom Sverige är därför främst FOI, universitet och tekniska högskolor.

Annat tekniskt stöd inom IT-säkerhetsområdet

Teknikkompetensfunktionen skall ses som samhällets resurs och ett komplement till marknaden inom området teknisk IT-säkerhet. Funktionen skall därför kunna stå till tjänst för samhället även med andra uppgifter än de ovan beskrivna om de har med teknisk IT-säkerhet att göra och där man av någon anledning inte kan vända sig till marknaden. I synnerhet gäller detta för ny teknik där samhällets behov av säkerhet inte säkert är automatiskt tillgodosett från början. Ett aktuellt exempel på ett sådant behov av säkerhet är de problem som kan uppstå med skydd av den personlig integriteten vid användning av IT.

Samhället kan ha behov av tekniska bedömningar av produkter och system, där målet inte är att skapa ett certifikat. Det kan t.ex. gälla en myndighet som, utan att ha behov att gå på djupet, vill ha en oberoende teknisk säkerhetsbedömning av ett system de vill köpa eller skapa själva. Ett annat exempel är funktionen för omvärldsanalys, som kan behöva tekniskt underlag för att kunna avgöra om man måste ompröva en hot- och sårbarhetsanalys inom någon samhällssektor. I de frågor där samhället behöver en teknisk IT-säkerhetsanalys skall teknikkompetensfunktionen kunna stå till tjänst med denna. Teknikkompetensfunktionen har en viktig roll att spela i att eliminera de tekniska sårbarheter som uppkommer i samhället undan för undan.

7.4.6 Organisatoriska överväganden

Teknikkompetensfunktionen kan efter en uppbyggnadsfas åtminstone delvis vara intäktsfinansierad. De flesta av funktionens uppgifter är sådana som utförs på uppdrag av en kund. Det är då en rimlig princip att kunderna står för kostnaderna att hålla de resurser som krävs för dessa uppgifter. Funktionen skall dock kunna utgöra en tillgänglig resurs vid kriser, varför den även behöver ha en viss anslagsfinansiering.

Teknikkompetensfunktionen bör inrättas i en miljö som är teknikorienterad för att ha förutsättningar att attrahera kvalificerad kompetens. Utredningen har funnit att FRA utgör en lämplig sådan miljö, varför utredningen förordar att teknikkompetensfunktionen organiseras i nära anslutning till FRA. Ytterligare fördelar med denna miljö är att FRA har en vana vid sekretess samt att FRA redan har några års erfarenhet på IT-säkerhetsområdet. Total-

försvarets myndigheter och andra myndigheter med särskilda säkerhetsbehov kan i dag anlita FRA som teknisk kompetens för att höja IT-säkerheten och förbättra sina skydd mot informationsoperationer. Vidare kan närheten till den kryptologiska kompetensen på FRA vara en fördel för funktionen.

Teknikkompetensfunktionen bör ges en från FRA organisatoriskt fristående ställning. Det är dock inte lämpligt att ge teknikkompetensfunktionen ställning som fristående myndighet. Den bör därför anknytas till en större myndighet som bör fungera som chefsmyndighet för teknikkompetensfunktionen. Utredningen har funnit två tänkbara alternativ till chefsmyndighet: FRA eller den av utredningen föreslagna planeringsmyndigheten. FRA har fördelarna att funktionen ändå enligt utredningens förslag kommer att placeras i dess närhet, och att FRA med sin erfarenhet på området kommer att ha goda förutsättningar att relativt snabbt etablera funktionen. Ett alternativ kan vara att låta den föreslagna planeringsmyndigheten bli chefsmyndighet. I så fall skulle man även få fördelen att planeringsmyndigheten lättare kan upprätthålla sitt övergripande ansvar över samhällets IT-säkerhet. Enligt utredningens uppfattning är dock fördelarna med FRA som chefsmyndighet övervägande. Utredningen förordar därför denna lösning.

7.5 IT-incidenthanteringsfunktionen

7.5.1 Allmänt

PTS fick 25 november 1999 i uppdrag av regeringen att utreda förutsättningarna för att inrätta en särskild funktion för IT-incidenthantering.¹⁶ Resultatet presenterades 28 november 2000 i rapporten *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering*.¹⁷ Näringsdepartementet remitterade rapporten 20 december 2000 till 76 instanser. I missivet framgick att PTS rapport med remissvar skulle överlämnas till Särbarhets- och säkerhetsutredningen för fortsatt beredning. Den IT-incidenthanteringsfunktion¹⁸ som utredningen föreslår har PTS rapport

¹⁶ Regeringsbeslut N1999/11654/ITFoU

¹⁷ PTS dnr 99-19448

¹⁸ En IT-incidenthanteringsfunktion kan ses som en CERT, vilket står för Computer Emergency Response Team. En svensk översättning saknas. Ordet CERT har använts så ofta att det blivit oklart exakt vad man förväntar sig av en CERT. Det är oklart vad som menas med *emergency*, i fråga om hur pass allvarlig en incident skall vara innan den anses vara uppgift för en CERT. Det är också oklart vad som menas med *response*, vilket kan tolkas som hela skalan från att avbryta den egna verksamheten och att reparera eventuella

som grund. Utredningen har gjort endast ett mindre antal justeringar av PTS förslag för att passa in det i det helhetsförslag som utredningen föreslår, och för att ta hänsyn till vissa av synpunkterna i remissvaren.

7.5.2 Motiv för ett statligt engagemang

Staten behöver ha en fungerande IT-incidenthantering. Funktionen för detta skulle i princip kunna upphandlas på den öppna marknaden. Det finns dock ett antal skäl som talar för att staten bör organisera denna funktion:

- Skydd mot informationsoperationer
- Brett samhällsintresse
- Officiell samverkan i internationella sammanhang

Skydd mot informationsoperationer

Funktionen kommer att hantera information som är sekretessmässigt känslig eller t.o.m. mycket känslig, varför förtroendet för funktionen måste vara orubbligt. Funktionen skall fullgöra uppgiften att föra statistik på de inkommande rapporterna. Statistiken skall analyseras för att kunna identifiera eventuella informationsoperationsattacker på bred front mot Sverige. Denna uppgift är säkerhetspolitiskt både så viktig och känslig att den inte utan vidare kan lämnas till privata aktörer.

Brett samhällsintresse

Målet är att funktionen skall kunna hantera IT-incidenter inte bara inom staten utan på sikt även inom kommuner, landsting och privata företag genom avtal. Det är rimligt att ett så brett åtagande över hela samhället organiseras av staten.

skador till att utföra motattacker. Noteras bör att man i dag internationellt har tonat ned "response"-aspekterna. Det är också, vilket inte är minst viktigt, oklart om en CERT skall anses ha operativa befogenheter eller ha endast varnande och rådgivande uppgifter. Eftersom dessa oklarheter finns används i denna text begreppet IT-incidenthanteringsfunktion, vilket även är termen i PTS rapport.

Officiell samverkan i internationella sammanhang

Sverige måste ha internationella kontakter med motsvarande instanser för IT-incidenthantering i andra länder. För att kunna upprätthålla den kompetens som krävs i sådana sammanhang och för att tillföra kunskaper i arbetet måste staten aktivt arbeta med IT-incidenthantering.

7.5.3 Krav på IT-incidenthanteringsfunktionen

Om IT-incidenthanteringsfunktionen skall kunna fullgöra sina uppgifter är det av avgörande betydelse att den skapar och upprätthåller ett stort antal kontakter på många områden såväl nationellt som internationellt. Funktionen måste sträva efter att bli medlem i välrenommerade IT-säkerhetsorganisationer, t.ex. The Forum of Incident Response and Security Teams (FIRST), som är en internationell paraplyorganisation för IT-incidenthanteringsfunktioner. Funktionen måste se till att ingå i nätverk där man sprider varningar och information om risker och sårbarheter. Funktionen måste ha en bred kännedom om aktörer på området i fråga om t.ex. forskning, utbildning, tjänster och produkter. För att inte riskera förtroendet för funktionen skall inte Polisen och Försvarsmakten delta i den, men funktionen måste ha goda relationer med dessa och andra myndigheter som på ett eller annat vis arbetar med IT-säkerhet. Utöver detta skall funktionen naturligtvis ha ett gott förhållande till alla sina kunder.

Både IT-incidenthanteringsfunktionen och teknikkompetensfunktionen skall utföra uppgifter som kräver teknisk kompetens. Det finns dock ett antal skillnader mellan de båda funktionerna, som principiellt kan sammanfattas i att för IT-incidenthanteringsfunktionen är tidsaspekten avgörande, medan för teknikkompetensfunktionen är den djupa tekniska kompetensen avgörande.

När det gäller tidsaspekten måste IT-incidenthanteringsfunktionen kunna reagera snabbt med varningar och tidskritisk rådgivning. Teknikkompetensfunktionen har inte detta krav på snabbhet, annat än i sin roll vid akut IT-kris hantering eller för att medverka till att ta fram motmedel mot nya elakartade program. IT-incidenthanteringsfunktionens fokus ligger därför på bredd och snabb tillgänglighet, medan de särskilt djupa tekniska kunskaperna utgör teknikkompetensfunktionens särdrag.

Tyngdpunkten i teknikkompetensfunktionens uppgifter kommer att vara kunduppdrag, medan IT-incidenthanteringsfunktionen kommer att ha en tyngdpunkt på hantering, rapportering och statistikföring av incidenter. Därmed finns också en skillnad i hur finansieringen skall ordnas. Teknikkompetensfunktionen blir lämpligen på sikt till stor del intäktsfinansierad, medan IT-incidenthanteringsfunktionen till större delen bör vara anslagsfinansierad.

7.5.4 Sammanfattning av förslagen i PTS rapport

PTS föreslår att en funktion för IT-incidenthantering inrättas på försök i två år i PTS egen regi. Funktionen skall i första hand betjäna de statliga myndigheterna. Huvuduppgiften skall vara att motverka angrepp på informations- och kommunikationstekniska system och infrastruktur inom den statliga sektorn. Funktionen skall ta emot och analysera incidentrapporter från myndigheterna. Varningar, råd och annan information skall kunna spridas till myndigheter, företag, organisationer och privatpersoner i Sverige. Funktionen skall också kunna samverka med enskilda organisationer inom IT-incidenthanteringsområdet.

Funktionens huvuduppgifter skall enligt PTS vara informationsförmedling, analys och samordning. Informationsförmedling skall i första hand ske på kontorstid, men funktionen bör ha möjlighet att förmedla varningar dygnet runt alla dagar på året.

PTS föreslår att funktionen bör ha beredskap dygnet runt alla dagar på året att medverka med samordning vid pågående IT-incidenter.

Funktionen måste för huvuduppgifterna ta emot incidentrapportering, göra informationsinsamling och statistik samt bedriva nationellt och internationellt samarbete. Funktionen bör kunna förmedla kontakter, utföra servicetjänster och medverka i utbildningar. Om tid medges bör funktionen också, enligt PTS, medverka i utvecklings- och standardiseringsarbete.

Funktionen bör enligt PTS bygga upp de bibliotek och databaser som behövs för verksamheten samt effektiva rutiner för arkivering av viktig IT-incidentrelaterad information.

PTS föreslår att funktionen skall beakta information om och analysera följande klasser av IT-incidenter:

- Intrångsförsök och dataintrång
- Avsiktlig störning av tillgänglighet

Datavirus och trojaner
Civila informationsoperationer
Informationsattacker
Nya typer av IT-incidenter

PTS föreslår att de rapporter funktionen tar emot om informationsattacker, efter eventuell sammanställning förmedlas vidare till i första hand SPF för analys. Formerna bör utformas av SPF och funktionen gemensamt.

PTS ser ingen möjlighet att ge funktionen operativa befogenheter utan författningsändringar, och ser inte heller något skäl till att ge funktionen några sådana befogenheter. Vidare föreslår PTS att polisen inte skall medverka i funktionen men att en god samverkan skall etableras. PTS föreslår att regeringen låter vidare utreda behovet av och formerna för en polisiär medverkan.

PTS har bedömt att nuvarande sekretesslagstiftning inte medger att myndigheter kan åläggas att rapportera incidenter till funktionen. PTS föreslår därför en frivillig rapportering under försöksperioden och att frågorna om rapporteringsplikt och behov av förändringar i sekretesslagstiftningen utreds vidare.

PTS föreslår att regeringen utreder och om så behövs utarbetar förslag till de författningsändringar som behövs för att underlätta brottsutredningar vid dataintrång.

7.5.5 IT-incidenthanteringsfunktionens uppgifter

Sårbarhets- och säkerhetsutredningen föreslår att IT-incidenthanteringsfunktionen skall betjäna samtliga statliga myndigheter. Dessutom skall kommuner, landsting och företag kunna ansluta sig till funktionen genom avtal.

Funktionen bör vara den naturliga instansen för sina kunder att vända sig till i frågor som rör information om IT-säkerhet och informationsoperationer, förebyggande arbete, åtgärder vid incidenter eller kontaktförmedling. Myndigheter och övriga anslutna organisationer skall till funktionen rapportera inträffade IT-säkerhetsincidenter. I gengäld sprider funktionen varningar, eventuellt tidskritiska,¹⁹ och ger återkoppling på det rapporterade materialet. Denna återkoppling kan bestå av statistik, risk- och hotbildsinfor-

¹⁹ Med tidskritiska varningar avses här sådana varningar som för att undvika risk för allvarliga skador på IT-system eller motsvarande, måste spridas även utanför ordinarie kontorstid.

mation eller bedömningar av enskilda inträffade säkerhetsincidenter.

Funktionen bör hantera dessa uppgifter:

- Ta emot incidentrapporter
- Larma och sprida varningar
- Ge aktiv tidskritisk rådgivning vid akuta IT-säkerhetsincidenter
- Föra statistik över IT-säkerhetsincidenter
- Sprida kunskap om IT-säkerhet och skydd mot informationsoperationer
- Ge råd och information om
 - åtgärder vid IT-säkerhetsincidenter
 - förberedelser för IT-incidenthantering
 - skyddsåtgärder
- Ge risk-, sårbarhets- och hotbildsinformation
- Förmedla kontakter
- Upprätta arkiv, bibliotek och databaser
- Standardisering av terminologi

Mottagande av incidentrapporter

Det finns åtminstone tre syften med en rapportering av IT-säkerhetsincidenter:

1. Den som rapporterar incidenterna kan erhålla hjälp med att bemöta dem.
2. Man rapporterar för att kunna varna andra.
3. Rapportering för statistik, som utgör ett väsentligt underlag t.ex. för att identifiera och urskilja samordnade attacker på bred front mot Sverige och nationella säkerhetsintressen.

Att ge hjälp vid säkerhetsincidenter och att varna är naturliga uppgifter för en IT-incidenthanteringsfunktion, varav följer att funktionen är en naturlig mottagare av incidentrapportering. Det är viktigt att funktionen för statistik på det rapporterade materialet. Statistiken kommer att vara en central informationskälla för att rätt kunna bedöma vilka insatser funktionen behöver göra. Statistiken kommer också att utgöra ett väsentligt underlag för att kunna identifiera samlade och systematiska angrepp mot Sverige.

Funktionen behöver inte nödvändigtvis vara den enda instans i samhället som tar emot incidentrapporter. Företag eller branscher kan välja att skapa egna CERT-organisationer. Detta behöver inte

vara en svaghet så länge alla dessa organisationer inklusive IT-incidenthanteringsfunktionen ingår i ett gemensamt nätverk där information och varningar kan utbytas utan onödigt dröjsmål. Det kan dessutom finnas fördelar med branschspecifika organisationer. Dels kan sådana organisationer ha bättre möjligheter att hjälpa sina kunder med de speciella problem som kan finnas i respektive bransch, dels kan det skapa bättre förutsättningar att få privata företag att ansluta sig.

På sikt finns det inte något hinder för att även den offentliga sektorn skall kunna välja mellan flera alternativa IT-incidenthanteringsfunktioner att ansluta sig till. I någon mening finns det redan i dag åtminstone två: CERT som Uppsala Universitet sedan år 2000 driver åt SUNET²⁰ för universitet och högskolor, tidigare vid Sunets driftcentral på KTH i Stockholm, samt ÖCB:s testverksamhet med rapportering av IT-incidenter där ett 50-tal myndigheter deltar. Emellertid, för att kunna fullgöra alla de uppgifter som grundar sig på en rapportering krävs att denna har en tillräcklig volym. Därmed bör i ett inledningsskede alla statliga myndigheter vara obligatoriskt anslutna till en gemensam IT-incidenthanteringsfunktion.

Det råder delade meningar om huruvida incidentrapportering skall vara obligatorisk eller frivillig för statliga myndigheter. Det viktigaste argumentet för ett obligatorium är problemet att volymen annars kan bli otillräcklig för att i tid kunna upptäcka en avancerad systematisk informationsattack mot Sverige. Utan en tillräcklig överblick kommer alla incidenter att framstå som sporadiska. Statistiken kommer därmed att bli bristfällig. Volymen är också viktig för att funktionen snabbt skall kunna utveckla kompetens på IT-incidenthanteringsområdet. Skulle funktionen till större delen tvingas öva sig på fiktiva incidenter riskerar man att förmågan blir lägre än önskvärt när en allvarlig verklig incident inträffar.

Erfarenheterna från ÖCB:s frivilliga testverksamhet är att volymen har varit mycket liten. Även om det är fullt möjligt att det förekommit endast få incidenter torde enligt utredningens uppfattning skälet till den låga volymen vara att alla incidenter inte har rapporterats eller ens upptäckts. ÖCB gör själva denna bedömning, grundad på att frivilligheten har medfört problem, men även att de flesta myndigheter saknar rutiner och organisation för intern IT-incidenthantering och att de därmed även har begränsade möjlig-

²⁰ SUNET (Swedish University Computer Network) är organisationen som driver de svenska universitetens och högskolornas gemensamma datanätverk

heter till upptäckt. Vi kan alltså inte med säkerhet veta om det i dag förekommer försök till systematiska attacker mot Sverige eller förberedelser till sådana.

Man skall visserligen ha klart för sig att ett obligatorium i sig inte utgör någon garanti för att volymen kommer att öka substantiellt. Ett allvarligt problem är ofta att myndigheter själva antingen inte upptäcker incidenter eller saknar fungerande interna rutiner för rapportering. Detta utgör dock inget argument mot ett obligatorium, utan pekar i stället på ett generellt behov av säkerhetshöjande åtgärder i form av ökad medvetenhet, högre kompetens, bättre teknik, tydligare organisation och klarare regler. Ett obligatorium kan medverka till att skapa incitament för myndigheter att etablera en god intern IT-incidenthantering och allmänt höja IT-säkerhetsnivån.

Ett argument för frivillig incidentrapportering är att ett obligatorium för statliga myndigheter kan vara juridiskt besvärligt, vilket PTS påtalar i sin rapport. Problemet ligger i sekretesslagen. Uppgifter som är sekretessbelagda inom en myndighet blir inte automatiskt sekretessbelagda inom en myndighet som delgivs dessa uppgifter. PTS förslag till lösning på problemet är att göra rapporteringen frivillig. Det går att lösa detta problem på annat sätt, nämligen genom att den rapporterande myndigheten gör en sekretessgranskning av de uppgifter som rapporteras och därmed ser till att inga hemliga uppgifter rapporteras. Även om rapporteringen därmed får något sämre kvalitet, blir inte kvantiteten mindre, vilket sannolikt i detta fall är av större betydelse. På sikt bör man dock via lagstiftning kombinerat med instruktion för IT-incidenthanteringsfunktionen garantera att rapporterade sekretessbelagda uppgifter även omfattas av sekretess hos funktionen. Med en sådan lösning kan man även erhålla bästa möjliga kvalitet på rapporteringen.

Ett annat argument för frivillig incidentrapportering är förtroendet. Genom att rapporteringen görs frivillig har man en garanti för att de som lämnar uppgifter verkligen gör det med förtroende. Det är onekligen så att ett förtroende för IT-incidenthanteringsfunktionen är av avgörande betydelse för att den skall kunna fullgöra sina uppgifter på ett tillfredsställande sätt. Förtroendet uppnås dock endast genom att funktionen visar i praktiken att den är värd ett förtroende. Funktionen får inte lämna ut uppgifter som kan identifieras till enskilda kunder. Funktionen måste kunna ge de rapporterade instanserna någonting värdefullt tillbaka. Funktionen får inte heller vara en polis. Skulle funktionen genom de

inrapporterade uppgifterna upptäcka brottslig eller misstänkt brottslig aktivitet mot en rapporterande organisation skall inte funktionen själv kontakta polisen. Funktionen skall i stället påtala det hela för den organisation som rapporterat och kan rekommendera denna att själv kontakta polisen. Detta kan möjligen kräva författningsändringar, men det är nödvändigt för förtroendet att funktionen inte gör polisanmälan av brott den får kännedom om genom rapportering. En obligatorisk incidentrapportering för statliga myndigheter kan visserligen skapa en svårighet för funktionen att i ett inledningsskede etablera detta förtroende, men denna svårighet bör inte vara oöverstiglig.

Det är svårt att komma runt behovet av en stor volym rapporterade incidenter för att upptäcka en avancerad samlad informationsattack mot Sverige. Detta argument får anses väga så tungt att det avgör frågan. Statliga myndigheter bör därmed åläggas att rapportera samtliga inträffade IT-säkerhetsincidenter till IT-incidenthanteringsfunktionen.

Privata företag och organisationer samt kommuner bör kunna ansluta sig och rapportera till funktionen på frivillig basis genom avtal. Ju fler som ansluter sig desto större underlag kommer funktionen att få för sina uppgifter. Detta understryker vikten av att funktionen agerar på ett sådant sätt att den inger ett stort förtroende. Företag måste kunna lita på att de behandlas med samma respekt som myndigheter och att sekretessen garanteras. Om funktionen genom lag, instruktion eller avtal är förbunden att inte lämna ut uppgifter om rapporterade incidenter till tredje part på ett sådant sätt att källan kan spåras, kan detta bidra till att stärka företagens möjligheter att ha förtroende för funktionen.

Larm och spridning av varningar

En central uppgift för funktionen är att kunna larma och sprida varningar om företeelser som kan hota IT-säkerheten. Det kan gälla nya virus eller andra elakartade program som kan utgöra hot eller störningsrisker för IT-system. Det kan gälla nya typer av störningar eller risk för störningar som någon råkat ut för. Det kan gälla intrångsförsök eller annan brottslig verksamhet som man kunnat identifiera t.ex. genom analys av incidentstatistik.

Uppgiften att larma är tidskritisk, åtminstone vad gäller att varna för nya virus eller andra elakartade program. Funktionens reaktionstid måste sålunda vara kort. Funktionen måste ha en

förmåga att snabbt kunna upptäcka nya elakartade program. Denna förmåga skapas dels genom att funktionen har en kanal för tidskritisk inrapportering som är öppen och bevakas dygnet runt, dels genom att funktionen prenumererar på varningar från CERT-organisationer och företag. Funktionen måste ha personal i jour. Vidare måste alla myndigheter och övriga organisationer som är anslutna till funktionen ha kanaler för att kunna ta emot de tidskritiska larmen.

Funktionen bör ha flera sätt att sprida varningar på. Varningar av allmängiltig karaktär bör publiceras på Internet. Anslutna organisationer bör få varningar sig direkt tillsända, särskilt de varningar som endast berör en eller ett fåtal organisationer. Särskilda kanaler bör användas för de tidskritiska larmen för att de säkert skall uppmärksammas.

Funktionen behöver inte alltid själv komma fram till vad som skall varnas om eller ta fram förslag till motåtgärder. Exempelvis kan funktionen för omvärldsanalys eller teknikkompetensfunktionen bidra i dessa sammanhang. Men det är viktigt att varningar och förslag till åtgärder kanaliseras genom IT-incidenthanteringsfunktionen, så att man får kontroll över att de rapporterade organisationerna får all återkoppling de skall ha.

Även i tidskritiska situationer måste funktionen beakta att organisationer lämnat uppgifter om sina incidenter till funktionen i förtroende. Innan varningar sprids måste funktionen se till att de uppgifter som lämnas ut inte kan härröras till den organisation som rapporterat uppgifterna. Om ett förtroende skulle brytas riskerar man att rapporteringen upphör, vilket skulle menligt inverka på funktionens möjligheter att fullgöra sina uppgifter.

Det är också viktigt att inte sprida falska varningar. Det finns många osanna rykten spridda om virus som påstås kunna orsaka omfattande skador på de system som drabbas. Dessa rykten sprids ofta med en uppmaning att sprida "varningen" vidare till så många som möjligt. Detta orsakar irritation och i värsta fall att nätverk, e-postserverar och andra datorer blir överlastade. Vidare skapas "vargen kommer"- effekten. När en verklig befogad varning kommer riskerar den att tolkas som ännu ett rykte. Skulle funktionen göra bedömningen att skaderisken blir för hög om man skulle vänta på att få en varning bekräftad innan den sprids vidare, måste varningen då kompletteras med information om att varningen ännu inte är bekräftad och uppgifter om hur man senare kan ta reda på aktuell status på varningen (sann, falsk eller obekräftad). Genom information på webbsidor skall funktionen också se till att

informera om varningar som är bekräftat falska utan att särskild information sprids via kanalerna för varning.

Aktiv tidskritisk rådgivning vid akuta IT-incidenter

Funktionen skall besitta en sådan kompetens att den vid inträffade IT-incidenter skall kunna ge stöd över telefon med rådgivning om akuta åtgärder. Information som funktionen kan ha genom andra organisationers rapportering om liknande incidenter eller genom kontakter med andra IT-säkerhetsorgan kan bidra till att funktionen eventuellt har bättre möjligheter än andra aktörer att överblicka situationen.

Ju högre kompetens en funktion har desto fler typer av incidenter kan den hantera. Som tidigare påpekats behöver dock inte funktionen ha kravet att kunna lösa djupare kundspecifika problem. Skulle det inträffa att en incident visar sig vara svårbemästrad p.g.a. t.ex. avsaknad av information eller att incidenten är tekniskt komplicerad, skall dock funktionen kunna hänvisa den rapportrande organisationen till aktörer med andra möjligheter att assistera. Aktörerna kan vara privata konsulter eller en statlig teknikkompetensfunktion. Med god kännedom om utbudet av tjänster behöver inte IT-incidenthanteringsfunktionen ha kravet att alltid själv besitta spjutspetskompetens inom alla områden av IT-säkerhet. Baskompetensen att kunna ge omedelbara generella råd måste dock vara ett minimikrav.

När IT-incidenthanteringsfunktionen väljer att hänvisa vidare måste det göras klart att det är den rapportrande organisationen själv och inte funktionen som fattar beslutet om vilken aktör den skall välja att anlita. Det skulle stå i direkt strid mot ansvarsprincipen om IT-incidenthanteringsfunktionen på eget initiativ skulle anlita t.ex. en statlig teknikkompetensfunktion för en rapportrande organisations räkning.

Statistik över IT-incidenter

Genom att föra statistik över rapporterade incidenter och över sådana incidenter man eventuellt fått kännedom om från andra källor, kan en IT-incidenthanteringsfunktion skapa underlag för analys av olika slag. Ett av de viktigaste syftena med en sådan statistik är att kunna avgöra om Sverige och nationella säkerhetsintres-

sen är utsatta för en bred och systematisk attack av informationsoperationer, eller för att finna indikationer på att en sådan attack håller på att förberedas. Detta är naturligtvis av säkerhetspolitiskt avgörande intresse.

Funktionen kan möjligen utföra någon egen analys av materialet och statistiken, men lär huvudsakligen rapportera statistiken vidare för analys hos andra instanser, t.ex. en funktion för omvärldsanalys. IT-incidenthanteringsfunktionen måste ha en dialog med avnämarna av statistiken för att dessa skall få ett underlag av hög kvalitet i rätt tid och med uppgifter av relevans för den analys som skall göras. Observera att funktionen inte kan lämna ifrån sig uppgiften att föra statistik eftersom uppgiften kräver tillgång till sekretessmässigt känsliga incidentrapporter som funktionen erhållit i förtroende. Statistiken får sålunda av en avnämare inte kunna kopplas till någon enskild rapporterande organisation. Funktionen bör dock själv kunna göra den kopplingen för att kunna återföra ett eventuellt resultat av analysen till de organisationer som berörs av resultatet.

Kunskapsspridning om IT-säkerhet och skydd mot informationsoperationer

Medvetenheten och kunskaperna om IT-säkerhet är inte alltid tillfredsställande överallt i samhället. Uppgiften att höja medvetenheten och kunskapsnivån är en av de allra viktigaste på kort sikt för att samhället skall kunna bli robustare och få en ökad IT-säkerhet. Ett robust IT-samhälle är också den viktigaste komponenten i ett gott skydd mot informationsoperationer.

Det är naturligt att IT-incidenthanteringsfunktionen är den centrala aktören i denna uppgift att höja medvetenheten och kunskapsnivån. Detta blir den logiska fortsättningen på funktionens uppgift att sprida varningar och ge allehanda rådgivning om IT-säkerhet. Det betyder dock inte att funktionen själv måste ta fram och sprida all information eller anordna alla slags utbildningar och seminarier om IT-säkerhet. Men funktionen bör ha en överblick över vad som finns och ha en uppgift att kanalisera informationen. Likaledes bör funktionen genom sin överblick uppmärksamma områden där utbudet av utbildning och information är bristfälligt. Genom sitt kontaktnät kan funktionen initiera förbättringar.

Rådgivning och information

IT-incidenthanteringsfunktionen bör ha i uppgift att informera och ge generella råd om IT-säkerhet till hela samhället. Funktionen bör ha skriftligt material om IT-säkerhet både i pappersform och publicerat på webbsidor. Funktionen skall även kunna ge enklare råd över telefon utöver den mer avancerade hjälp vid akuta IT-säkerhetsincidenter som funktionen kan ge eller förmedla till myndigheter och de företag och organisationer som man har avtal med.

Funktionen behöver inte nödvändigtvis själv ta fram de råd man förmedlar, utan kan med fördel ta hjälp av expertis från andra instanser. T.ex. kan teknikkompetensfunktionen bistå med att ta fram råd om teknisk IT-säkerhet. IT-incidenthanteringsfunktionen skall dock kunna förmedla alla typer av råd och se till att de finns lättillgängliga.

Funktionen skall kunna ge generella råd om lämpliga åtgärder vid olika slag av IT-incidenter. Exempel kan vara åtgärder vid virusangrepp, åtgärder vid misstänkta intrångsförsök eller åtgärder vid tillgänglighetsattacker.²¹ Råden skall gälla både hur man kan avbryta en pågående incident samt hur man kan lindra effekterna av den och restaurera efter den. Råden skall vara utformade så att åtgärderna inte försvårar för en eventuell polisutredning om incidenten beror på brottslig verksamhet.

Funktionen skall kunna ge generella råd om lämpliga förberedelser för att kunna hantera de IT-incidenter som kan uppstå. Råd skall ges om vilka förberedelser man skall göra för att kunna upptäcka incidenter, t.ex. att alltid ha uppdaterade antivirusprogram och att ha rutiner för logganalys. Råd skall ges om vilka förberedelser man kan göra för att lindra skadeverkningarna av incidenter, t.ex. att ha säkerhetskopior av väsentliga data och att ha reservsystem till de system som inte får ha långa avbrott i driften.

En viktig del i förberedelserna är att ta fram och underhålla organisation och regler för den egna IT-säkerheten, eller i ett vidare perspektiv informationssäkerheten. Man måste ta fram säkerhetspolicy, säkerhetsorganisation med ansvarsfördelning, rutiner för val av personal, drifrutiner, rutiner vid inträffade IT-incidenter m.m. En IT-incidenthanteringsfunktion skall kunna ge råd om vad man behöver ta fram för dokument och hur de skall utformas.

²¹ Tillgänglighetsattacker kallas även DoS-attacker, där DoS är en förkortning för *Denial of Service*. Begreppet innebär att en angripare förhindrar legitima användare att använda sina datorer, vanligtvis genom att skicka så pass mycket trafik till dem att volymerna överskrider datorernas kapacitet, vilket medför att de kollapsar

Funktionen skall kunna ge generella råd om skyddsåtgärder genom teknik, organisation eller regler. Exempel på vad funktionen skall kunna ge råd om är vad man bör tänka på när man ansluter sig mot Internet, vilka säkerhetsåtgärder man bör vidta vid installation av olika programvaror eller exempel på olika policyn man kan ha med för- och nackdelar rörande personalens möjlighet att kryptera filer.

Risk-, sårbarhets- och hotbildsinformation

En viktig uppgift för IT-incidenthanteringsfunktionen är att förmedla tillgänglig information om risker, sårbarheter och hotbilder på IT-området. Funktionen skall se till att aktuell information finns tillgänglig och att den delges dem som berörs av informationen. I den mån informationen inte är sekretessbelagd skall den även publiceras. Informationen om hotbilder, dvs. vilka aktörer som kan utgöra ett hot och varför, skall vara anpassad till flera olika kundkretsar såsom privatpersoner, enskilda företag, branscher, myndigheter eller hela staten. Informationen om sårbarheter kan t.ex. omfatta kända problem med olika IT-produkter eller problem som kan uppstå med bristande organisation, rutiner och regelverk.

Kombinationen av information om hotbild, sårbarheter och konsekvenser av ett fullföljt angrepp är en riskbedömning. En sådan kan vara möjlig att göra exempelvis om man vid analys av rapporterade incidenter kan identifiera systematiska försök till angrepp. En IT-incidenthanteringsfunktion skall kunna förmedla information om aktuella riskbedömningar.

IT-incidenthanteringsfunktionen behöver inte nödvändigtvis själv utföra den analys som ligger till grund för informationen, utan kan med fördel erhålla informationen från en funktion för omvärldsanalys. Det är dock viktigt att IT-incidenthanteringsfunktionen kan förmedla den information som finns.

Kontaktförmedling

En viktig uppgift för IT-incidenthanteringsfunktionen är att ha en aktuell förteckning över olika aktörer inom IT-säkerhetsområdet. Det kan gälla att veta vilket ansvar eller vilken kompetens olika myndigheter har inom området, vilka företag som kan erbjuda

olika tjänster, eller vilka svenska och utländska organisationer som agerar i olika sammanhang på området. Funktionen skall kunna förmedla denna information och gärna själv stimulera till att lämpliga kontakter skapas mellan olika aktörer. Funktionen bör naturligtvis själv sträva efter att ha ett så brett kontaktnät som möjligt, såväl inom som utom landet.

Arkiv, bibliotek och databaser

En naturlig del i IT-incidenthanteringsfunktionens informationsförmedlande roll är att skapa och upprätthålla arkiv, bibliotek och databaser med all slags information om IT-säkerhet och informationsoperationer. Det kan gälla information om sårbarheter och inträffade incidenter, artiklar i ämnet eller länkbibliotek till olika aktörer. Funktionen kommer att behöva informationen för sitt interna arbete. Den information som inte är sekretessbelagd bör även vara tillgänglig för allmän sökning i så stor omfattning som möjligt.

Standardisering av terminologi

PTS föreslår i sin rapport att IT-incidenthanteringsfunktionen skall kunna delta i framför allt internationellt arbete med att standardisera terminologi vad avser IT-incidenter, sårbarheter, m.m. Sårbarhets- och säkerhetsutredningen tillstyrker detta. Fördelen med att ge en IT-incidenthanteringsfunktion denna uppgift är att funktionen ändå måste etablera lämpliga kontakter i de internationella forum där terminologin standardiseras. Dock måste det röra sig om att delta i arbetet och inte att leda det. Andra instanser i samhället kan vara mer lämpade för detta, såsom Informations-tekniska standardiseringen (ITS) eller möjligen Terminologicentrum (TNC).

7.5.6 Förändringar jämfört med PTS rapport

Till största delen sammanfaller de av Sårbarhets- och säkerhetsutredningen föreslagna uppgifterna med de uppgifter som PTS föreslår. Vissa skillnader finns dock. Dessa kommenteras i det följande.

Kundspecifik rådgivning

Det är å ena sidan bra om IT-incidenthanteringsfunktionen kan klara av många typer av frågor om IT-säkerhet. Å andra sidan skall dubbelarbete undvikas. I och med att en teknikkompetensfunktion inrättas behöver inte IT-incidenthanteringsfunktionen ha kravet att kunna åta sig att ge djup kundspecifik rådgivning avseende vare sig preventiva eller akuta åtgärder vid IT-incidenter. Sådan rådgivning kommer att kräva ingående analys och särskild kompetens för att kunna lösas på bästa sätt, varför teknikkompetensfunktionen är bättre lämpad att hantera denna rådgivning. Oaktat detta måste IT-incidenthanteringsfunktionen ha en sådan bred kompetens att den snabbt kan ge generella råd om åtgärder vid inträffade incidenter eller förslag på lämpliga skyddsåtgärder.

Forskning och utveckling

Forskning och utveckling bör företrädesvis bedrivas av andra instanser, såsom FOI och högskolor. En annan sak är att en IT-incidenthanteringsfunktion lämpligen har goda kontakter med forskare och institutioner där forskning och utveckling bedrivs.

Hotbildsanalys

IT-incidenthanteringsfunktionen har en viktig uppgift att analysera inträffade incidenter för att kunna urskilja systematiska och kvalificerade angrepp. Funktionen behöver också analysera incidenter för att på bästa sätt kunna fullgöra sina uppgifter att varna och ge omedelbar hjälp.

För att fullständigt kunna identifiera systematiska och kvalificerade angrepp och för att kunna komplettera till en hotbildsanalys, krävs dock ytterligare information från bl.a. underrättelsetjänst. Funktionen kommer att sakna sådan information, varför den analys funktionen utför med ett bearbetat underlag måste ges vidare till funktionen för omvärldsanalys och till det tvärsektoriella samordningsorganet. Endast i dessa instanser kan man ha tillräckligt underlag för att kunna utföra djupare analys och bearbetning och därmed säkert kunna uppfatta förändringar i hotbilden. I och med att dessa instanser får utföra den djupare analysen löser man också ett problem som någon remissinstans påpekat, att man inte bör blanda analys med operativ verksamhet.

Samordning vid pågående IT-incidenter

Att samordna vid pågående IT-incidenter faller naturligt på ett tvärasektoriellt samordningsorgan, varför uppgiften formellt sett inte skall äläggas IT-incidenthanteringsfunktionen såsom PTS föreslår. Men samordningsorganet bör å andra sidan utnyttja det kontaktnät som IT-incidenthanteringsfunktionen faktiskt kommer att ha. IT-incidenthanteringsfunktionen kommer därför sannolikt i praktiken, om än inte formellt, att bidra till samordningen på det sätt PTS föreslår.

Utvecklingsperiod

PTS föreslår att IT-incidenthanteringsfunktionen inrättas på försök i två år. De flesta remissinstanser har samtyckt till detta. Några har dock anfört farhågor att detta dels kan leda till att funktionen inte kommer att kunna rekrytera kompetent personal, dels att funktionen kommer att bli omöjlig att utvärdera. Sårbarhets- och säkerhetsutredningen finner att dessa farhågor väger tungt. Samtidigt kan man konstatera att en överväldigande majoritet av remissinstanserna tillstyrker att en IT-incidenthanteringsfunktion inrättas. Det är därför osannolikt att en försöksperiod skulle följas av att funktionen läggs ner. Internationella jämförelser tyder inte heller på detta. Därför föreslår utredningen att funktionen inrättas permanent, med en utvecklingsperiod på två år, efter vilken en utvärdering av funktionen genomförs.

Några remissinstanser har föreslagit att en referensgrupp inrättas, sammansatt av representanter från myndigheter med kompetens på IT-säkerhetsområdet. Gruppens uppgift skall vara att följa funktionen och att efter utvecklingsperioden utvärdera den efter på förhand angivna kriterier. Sårbarhets- och säkerhetsutredningen samtycker till detta förslag.

Frivillig eller obligatorisk incidentrapportering

PTS finner att nuvarande sekretesslagstiftning inte medger en rapporteringsplikt, och föreslår i stället att myndigheter rapporterar frivilligt under de första två åren. Under den tiden kan behovet av en plikt och möjligheterna till författningsändringar utredas. En majoritet av de remissinstanser som tar upp frågan anser att en rapporteringsplikt vore önskvärd. Sårbarhets- och säkerhetsutred-

ningen instämmer med dessa remissinstanser, och föreslår därför att en rapporteringsplikt för samtliga statliga myndigheter införs redan från början. För att inte en sådan plikt skall strida mot sekretesslagen medan den ses över och eventuellt revideras, kompletteras plikten med att respektive myndighet sekretessgranskar de detaljer som lämnas ut om inträffade incidenter. Detta kan medföra att kvaliteten på rapporteringen inledningsvis blir något sämre, men inte kvantiteten.

Typ av IT-incidenter som skall hanteras

PTS föreslår att IT-incidenthanteringsfunktionen skall beakta IT-incidenter som innebär angrepp, dvs. intrångsförsök och dataintrång, avsiktlig störning av tillgänglighet, datavirus och trojaner, civila informationsoperationer, informationsattacker samt nya typer av IT-incidenter.

Flera remissinstanser har haft synpunkter på detta. En del har befarat att detta kommer att innebära att alltför många incidenter skall behöva rapporteras. Man har önskat en begränsning som gör att t.ex. enkla virus som stoppas av antivirusprogram inte skall behöva rapporteras. Några har även funnit terminologin främmande.

Sårbarhets- och säkerhetsutredningen föreslår att man inför begreppet IT-säkerhetsincident. Denna term är hämtad från en magisteruppsats av Jimmy Arvidsson,²² i vilken bl.a. föreslås en enhetlig terminologi inom området IT-incidenthantering. Begreppet IT-säkerhetsincident definieras där som en händelse som är säkerhetskritisk för IT-verksamheten.

Med denna begränsning av de incidenter som skall rapporteras kommer inte mindre allvarliga händelser att omfattas, såsom virus som stoppas av antivirusprogram. Därigenom uppnås att funktionen slipper en onödig arbetsbelastning och att man eliminerar information som kan vara störande vid en analys. Man kommer däremot att inkludera IT-incidenter som kan vara säkerhetskritiska utan att man för den skull har kunnat avgöra om de beror på brottslig verksamhet eller ej. Sådana händelser kan vara nog så viktiga att få med i en nationell statistik.

²² Jimmy Arvidsson: *Incidentorganisation och incidenthantering*. Stockholms Universitet DSV/KTH 1999–2000.

7.5.7 Organisatoriska överväganden

PTS föreslog i sin rapport att IT-incidenthanteringsfunktionen skulle organiseras av PTS. För att kunna ge funktionen bästa förutsättningar att garantera sekretessen på de inrapporterade incidenterna har dock utredningen funnit att funktionen bör ges en fristående ställning. Utredningen anser vidare att funktionen bör organiseras i högskolemiljö med teknisk kompetens. Därigenom skapas goda förutsättningar för funktionens kompetensförsörjning.

Funktionen kommer inte att bli tillräckligt stor för att motivera att den blir en fristående myndighet under något departement, varför den bör ha en chefsmyndighet. Det finns flera tänkbara myndigheter som skulle kunna vara chefsmyndighet. PTS har genom att utreda förutsättningarna för funktionen även en hög beredskap för att relativt snabbt bygga upp funktionen. Planeringsmyndigheten kommer att ta med sig erfarenheterna av ÖCB:s försök med incidentrapportering. Utredningen anser dessa vara de två främsta alternativen. Utredningen anser att det är viktigt att funktionen byggs upp snarast möjligt, och finner att PTS med sin beredskap inför uppgiften därför har bäst förutsättningar att vara chefsmyndighet.

Det bör påpekas att flera remissinstanser har förordat andra lösningar än att låta PTS organisera funktionen. Även om funktionen blir en egen myndighet, finns ändå en koppling till PTS, om än svag, med PTS som chefsmyndighet. Därför föreslår utredningen att IT-incidenthanteringsfunktionen utvärderas efter två års utveckling, och att i denna utvärdering ingår en förutsättningslös prövning av huvudmannaskapet.

7.6 Omvärldsanalysfunktionen

Ett effektivt IT-säkerhetsarbete förutsätter att man noga följer utvecklingen i omvärlden och analyserar dess konsekvenser för IT-säkerheten. Bevakning bör inte endast inriktas på IT-relaterade frågor utan också avse samhällsutvecklingen i stort samt områden som är beroende av en fungerande IT-verksamhet. Det är också väsentligt att den tekniska utvecklingen inom IT-området bevakas noga i syfte att skapa beredskap att möta inslag i utvecklingen som kan ge upphov till nya typer av IT-hot. Den tekniska utvecklingen bör därför fortlöpande analyseras från säkerhetssynpunkt. Bevak-

ningen bör särskilt uppmärksamma allvarliga händelser såsom informationsoperationer.

Det bör vara en naturlig del av omvärldsanalysfunktionens verksamhet att följa utvecklingen på Internet. Detta bör ske i syfte att identifiera och bedöma företeelser, trender och aktiviteter som kan bidra till att fördjupa omvärldsanalysen i stort. Detta är motiverat med hänsyn till att Internet på kort tid har framträtt som ett nytt väsentligt informationsmedium vid sidan av andra medier som tidningar, radio, TV och litteratur.

En kvalificerad omvärldsbevakning är resurskrävande. Det är nödvändigt att följa utvecklingen inom en rad specialområden genom egna analyser eller genom att ta del av analyser som görs av andra. Den snabba tekniska utvecklingen medför dessutom att genomgångar av utvecklingen inom ett delområde måste upprepas relativt ofta för att inte bli inaktuella. Det är också angeläget att ha ett omfattande samarbete med analysfunktioner hos organ inom och utom landet som arbetar med liknande frågor. Detta är ett sätt att stämna av och kvalitetssäkra de bedömningar som görs.

Av dessa skäl är det inte lämpligt att bygga upp en fristående omvärldsanalysfunktion inom IT-säkerhetsområdet. Omvärldsanalysfunktionen inom detta område bör därför integreras i den omvärldsanalysfunktion som föreslås i kapitel 5. Man kan då ta tillvara de synergieffekter som uppstår, t.ex. vid den generella bevakningen av samhällsutvecklingen och den tekniska utvecklingen inom infrastrukturområdet. Synergieffekter bör också finnas i den internationella kontaktverksamheten.

Med dessa förutsättningar kan omvärldsanalysfunktionen inom IT-säkerhetsområdet ha en relativt liten fast personalstyrka. Det torde också vara värdefullt för planeringsmyndighetens övriga omvärldsbevakning att ha nära kontakt med omvärldsbevakningen inom IT-säkerhetsområdet. Enligt utredningens förslag skall planeringsmyndigheten också vara IT-säkerhetsmyndighet och fungera som sekretariat till det IT-säkerhetssamordningsorgan som utredningen föreslår inom Regeringskansliet. Detta är ytterligare ett motiv till varför omvärldsanalysfunktionen inom IT-säkerhetsområdet bör kopplas till planeringsmyndigheten.

7.7 Ett system för certifiering av IT-produkter

7.7.1 Bakgrund

Problemen med sårbarheten i samhällets informationssystem uppmärksammas i nyhetsmedier i sort sett varje dag. Rapporterna kan röra sig om intrång i kommersiella system för Internet-tjänster, avancerat spionage i industrins utvecklingsmiljöer eller omfattande hackerangrepp via manipulerade hemdatorer. Hotet från informationsoperationer belyser ytterligare sårbarhetsfrågorna för särskilt kritiska system i infrastrukturen, men också den "horisontella" störning som kan uppstå vid attacker riktade mot ett stort antal mål inom en eller flera samhällssektorer.

Certifiering av IT-säkerhet med stöd av internationellt accepterade standarder är ett viktigt område för att skapa tillit och förtroende såväl inom en organisation som mellan olika parter. Certifiering berör i huvudsak två ISO/IEC-standarder. Den första, ISO/IEC IS 15408, *Evalueringskriterier för IT-säkerhet*, också kallad *Common Criteria*, behandlar grunden för certifiering vad gäller granskning och evaluering av teknisk IT-säkerhet (produkt- och systemcertifiering). Den andra rör certifiering av ledning av informationssäkerheten i en organisation. Sedan 1999 finns en svensk standard, SS 62 77 99, *Ledningssystem för informationssäkerhet*, som är en svensk bearbetning av den internationella standarden IS 17799, *Code of practice for information security management*. När det gäller åtgärder för att höja säkerheten i vid bemärkelse i samhällets användning av IT är viktigt att satsa resurser på såväl grundläggande teknisk IT-säkerhet som säkerhet i organisationers användning av informationssystem. I detta avsnitt behandlas inte närmare certifiering av ledningssystem för informationssäkerhet.

För att kunna granska säkerheten i en produkt eller i ett system krävs en beskriven metodik. Alltför många fall i verkligheten visar på hur man annars i en informell teknisk granskning i efterhand lätt råkar ut för stora svårigheter att påvisa vad som granskningen omfattat och vilken metodik som egentligen tillämpats. Ofta uppstår också brister i dokumentationen av den informella processen.

Säkerhetsfunktioner i olika systemkomponenter måste fungera väl och ha motståndskraft mot direkta attacker. Den totala uppsättningen säkerhetsfunktioner måste också vara tillräcklig för att kunna avbilda verksamhetens regler för åtkomstkontroll, identifiering, loggning, larm etc. Helheten i säkerhetslösningarna är här

väsentlig; säkerhetsfunktionerna i systemet måste tillsammans (också i inbördes samverkan) kunna etablera ett fungerande skydd.

7.7.2 Behovet av tillit

En fortlöpande höjning av säkerheten i informationssystem och nätverk är en grundförutsättning för det framtida informations-samhället. Användarna är beroende av säkerhetsegenskaperna hos de produkter som används för att bygga upp olika system. Dessa egenskaper rör dels förekomsten av de säkerhetsfunktioner som behövs för att uppfylla önskade regler och policy, dels tillit till eller förtroende för att dessa funktioner verkligen fungerar och har en tillräcklig motståndskraft mot attacker.

Fackbegreppet för måttet på detta förtroende är assurans. Åtgärder för att skapa detta kan normalt inte hanteras inom den egna organisationen. Få organisationer har resurser och kompetens för att kunna bedöma säkerheten i de produkter man avser att använda. Man är här beroende av generella, gemensamma åtgärder. Detta gäller i första hand åtgärder som syftar till att reducera sannolikheten för förekomsten av svagheter som någon kan utnyttja i de tekniska lösningarna. Åtgärderna höjer därmed säkerheten i dessa tekniska lösningar. Granskning av de tekniska säkerhetsegenskaperna kallas normalt evaluering. Denna typ av granskning sker i många länder av oberoende tredje part; särskilt godkända och ackrediterade företag.²³ Resultaten fastställs av certifieringsorgan som även har till uppgift att, ofta tillsammans med det nationella ackrediteringsorganet, övervaka evalueringsföretagen vad gäller deras rutiner, metoder och kompetens. I många länder är även certifieringsorganen själva ackrediterade av den nationella ackrediteringsmyndigheten.

I regeringens proposition *Ett informationssamhälle för alla*²⁴ framhålls vikten av ett fördjupat arbete kring frågor som rör skydd mot informationsoperationer, säkrare Internet, elektroniska signaturer och annan säkerhetsteknik. Insatserna skall inriktas mot att skapa förtroende för den nya tekniken genom att bidra till bättre generella förutsättningar för informationssäkerhetsarbetet. Vidare fäster regeringen stor vikt vid de internationella frågorna i informationssäkerhetsarbetet. Sverige skall även i framtiden ha en aktiv roll i det internationella arbetet med dessa frågor.

²³ På engelska "IT Security Evaluation Facilities"; ITSEF

²⁴ Prop. 1999/2000:86

Ett viktigt exempel på internationell samverkan är i detta sammanhang den under 2000 tillskapade internationella överenskommelsen för erkännande av IT-säkerhetscertifikat (Recognition Arrangement for IT Security Certificates) baserade på IS 15408.

Syftet med denna överenskommelse är att tillse

att evalueringar utförs enligt en väldefinierad, internationellt accepterad standard

att evalueringsresultat allmänt upplevs som att kraftfullt bidrag till förtroende för säkerheten i granskade produkter

en förbättring av tillgången till evaluerade, säkerhetsförstärkta produkter

att man eliminerar dubblering av kostnader för upprepade evalueringar i olika länder

att man kontinuerligt förbättra effektivitet och kostnadsbild för evaluerings- och certifieringsprocesserna.

Bland undertecknarna finns i dag representanter från fjorton av de ledande industriländerna. Bland dessa finns dels länder som redan i dag har egna procedurer för evaluering och certifiering,²⁵ dels sådana som f.n. saknar sådana men som likväl har ett berättigat intresse av insyn i hur certifiering går till och de inom gruppen tillämpade metoderna för inbördes inspektion av certifieringsorganen i respektive land. Sverige har ännu inte undertecknat denna överenskommelse. Sårbarhets- och säkerhetsutredningen anser att Sverige utan dröjsmål skall underteckna överenskommelsen. Delta-gandet torde ligga väl i linje med regeringens uttalanden om vikten av internationell samverkan inom IT-säkerhetsområdet.

7.7.3 Utvecklingen i omvärlden

Idealt borde säkerheten i ett IT-system testas genom att utsätta det för varje tänkbar kombination av indata eller insignaler och samtidigt observera om säkerheten vid något tillfälle åsidosatts. Detta kallas uttömmande testning, vilket i praktiken är omöjligt att utföra p.g.a. de ofantligt många kombinationer av indata eller insignaler som normalt finns.

Andra vägar måste därför prövas. Under slutet av 1960-talet och början av 1970-talet genomförde det amerikanska försvaret ett

²⁵ Beskrivning av ett stort antal länders system för evaluering och certifiering redovisades vid den första internationella konferensen för IS 15408 (*Common Criteria*) i Baltimore, USA maj 2000. Se <http://niap.nist.gov/cc-scheme/iccc/tracka-nj.html>

större antal framgångsrika intrångsförsök (aktiv IT-kontroll eller s.k. *Red Team*-operationer) mot egna system. Det framgick snart att inriktningen att (enbart) försöka rätta till efterhand upptäckta svagheter inte var en framgångsrik väg.²⁶

I stället initierades ett forskningsprogram som ledde fram till följande slutsatser. Den säkerhetskritiska delen av systemet:

- måste vara väl isolerad och modulariserad dvs. finnas i en väl definierad, isolerad och separat fungerande enhet så att den går att granska,
- måste ha en del som har ansvar för alla åtkomstbeslut,
- måste alltid vara aktiv,
- får inte kunna kringgås.

För att kunna uppnå detta föreslogs ett antal kriterier (på olika noggrannhetsnivåer) som definierade de olika granskningsåtgärderna.²⁷ En liknande utveckling följde i Europa och Kanada.²⁸ Det gemensamma syftet var att främja en utveckling av kommersiella säkerhetsprodukter (inklusive traditionella produkter med ingående säkerhetsfunktioner) som bättre kunde möta säkerhetsmedvetna köparens krav på säkerhet.

En fokusering på försök att påvisa och korrigera existerande svagheter är med andra ord otillräcklig som metod för att komma till rätta med de grundläggande problemen. I stället måste konstruktion och uppbyggnad av säkerheten genomföras på ett konsekvent och genomtänkt sätt. Kriterier för granskningsåtgärder har inriktats mot krav på undersökning av konstruktionsprinciper och genomförande. Säkerställande av spårbarhet från identifierade hot och säkerhetsbestämmelser till framtagna säkerhetsfunktioner och mekanismer har blivit en central del av arbetet. Som en del av granskningen genomförs ibland även intrångstester, i första hand för att påvisa att funna brister kan utnyttjas i praktiken.

Granskningen innebär således att en part, utvecklaren, skall kunna övertyga någon annan, granskaren (evalueraren) att konstruktion i fråga om principer och övergripande lösning samt reali-

²⁶ Denna inriktning (kallas i USA *Penetrate and Patch*) används med fördel för att påvisa existerande svagheter i produkter och konfiguration och är i samband med övningar ett effektivt hjälpmedel för att öka driftpersonalens uppmärksamhet och förståelse. Upptäckta och publicerade svagheter bör alltid snarast åtgärdas eftersom dessa ofta utnyttjas som grund för angrepp. Metoden kan däremot inte användas för att bevisa att ett system är säkert

²⁷ *Trusted Computer System Evaluation Criteria*; TCSEC; 1983. US-MIL-STD 5200.28, 1985.

²⁸ I Europa, *IT Security Evaluation Criteria* (ITSEC), 1990, 1992. I Kanada, *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC), 1990, 1991

sering svarar mot i förhand fastställda granskningskrav. Ambitionen har varit att leverantörerna skall lägga ökad vikt vid omsorgsfull design av säkerheten i tidigt skede av utvecklingen som en lönsam och effektiv väg mot bättre säkerhetsegenskaper. Ur användarnas synvinkel handlar evaluering om att skapa ett mått på önskvärt förtroende och tillit som ett sätt att reducera sannolikheten för kvarstående svagheter som kan utnyttjas, och därmed reducera riskerna.

Tidigare i huvudsak militärt inriktade regler och bedömningskriterier har i dag ersatts av kommersiellt orienterade system för evaluering (teknisk säkerhetsgranskning) och certifiering. Arbetet som bedrivits genom internationellt samarbete, syftade till att ersätta de tidigare nationella eller regionala regelverken med en gemensam standard. Under 1999 fastställdes den nya internationella standarden IS 15408, *Evalueringskriterier för IT-säkerhet (Common Criteria)*.

Evaluering innebär att en oberoende part granskar konstruktion och dokumentation enligt fastställda granskningskriterier. Dessa granskningskriterier kan ha olika nivåer. Som exempel kan nämnas att i IS 15408 finns sju fördefinierade nivåer som definierar granskningsåtgärder med successivt ökande krav. Den lägsta nivån innebär mycket begränsade åtgärder såväl vad gäller leverantörens underlag som insatsen för evaluering och certifiering. Evalueringar på denna nivå kan genomföras på kort tid. Höga nivåer kräver större insatser och kan, i synnerhet för komplicerade produkter, ta tämligen lång tid. Genom att erbjuda sju olika nivåer kan användare av standarden hos leverantörer respektive upphandlande enheter på kundsidan välja en lämplig nivå med hänsyn till marknadsbehov, kostnader och risker.

Under perioden 1988–1991 formulerade Storbritannien, Frankrike, Tyskland och Nederländerna gemensamt nya kriterier för evaluering av IT-säkerhet (*IT Security Evaluation Criteria; IT-SEC*), vilka rekommenderades av EU:s Ministerråd i en rekommendation i april 1995. Arbetet fokuserades på specifikation av granskningskraven och skilde sig gentemot de tidigare amerikanska kriterierna främst genom att inte längre vara inriktade mot operativsystem för fleranvändarsystem samt genom att förutsätta att granskningen kunde genomföras effektivare och snabbare än tidigare. Det senare åstadkoms genom att tydliggöra dokumentations- och granskningsåtgärderna samt genom att lita till oberoende evalueringsföretag. Däremot lämnades frågan om hur krav på säkerhetsfunktioner (funktionalitet) skulle uttryckas utanför.

Under 1990-talet har Kanada, USA, Storbritannien, Frankrike och Tyskland (inledningsvis även Nederländerna) gemensamt tagit fram underlag för en internationell uppsättning kriterier.²⁹ Arbetet har bedrivits i nära samverkan med internationella standardiseringsorgan (ISO/IEC) och ledde 1999 fram till IS 15408. Ett stort antal länder tillämpar i dag denna standard på nationell nivå. Ett antal ledande länder (USA, Kanada, Storbritannien, Tyskland, Frankrike m.fl.) ingår i den aktiva gruppen.

Arbets sättet i Europa har inneburit att leverantören själv genom avtal med något godkänt evalueringsföretag arrangerat evaluering av sin produkt. USA har nu byggt upp ett liknande system (NIAP – *National Information Assurance Program*). För att möta risken för att evalueringsföretaget kommer under ekonomiskt tryck från leverantören att avge en positiv rapport låter man ett certifieringsorgan granska evalueringsresultatet och först därefter ge ut ett certifikat samt utöva tillsyn över evalueringsföretaget så att det arbetar med godkänd metodik och med erforderlig kompetens. Evalueringsföretaget måste även kunna upprätthålla en hög sekretessnivå vad gäller företagshemliga konstruktionsdetaljer som granskarna i vissa fall behöver kunna ta del av.

Till skillnad mot tidigare nationella och regionala kriterier innefattar den nya standarden även ett bibliotek över kravkomponenter för ett stort antal olika funktionsegenskaper (för säkerhetsfunktioner) vilket avsevärt underlättar och förstärker specifikationsprocessen när det gäller att uttrycka verifierbara krav på säkerhetsfunktionerna.

En utveckling har också inletts där intressenter och organisationer på kundsidan utvecklar generella kravprofiler för olika produkttyper (s.k. skyddsprofiler – *Protection Profiles*). Härigenom förväntas utvecklingen mot en bättre avpassad säkerhet i olika IT-produkter främjas. Upphandlingar kan där så är lämpligt enkelt referera till önskad skyddsprofil. Leverantörernas arbete med att beskriva egenskaperna hos sina produkter enligt standardens krav (Security Target) underlättas också.

²⁹ Till skillnad mot tidigare förfarande i USA (med evaluering utförd av myndighet) har man satsat på att speciellt godkända evalueringsföretag (IT Security Evaluation Facility; ITSEF) skall utföra evalueringen, normalt på uppdrag av utvecklaren/leverantören. Resultatet granskas sedan av en separat, oberoende certifieringsfunktion som kontrollerar att granskningen skett med fastställd metodik och kompetens. Certifieringsfunktionen ger därefter ut ett certifikat som bevis på detta – till stöd för marknaden.

7.7.4 Utvecklingen i Sverige

Området certifiering av IT-säkerhet har analyserats av ett antal utredningar och projekt under 1990-talet.³⁰ Arbetet har bedrivits mot bakgrund av den pågående internationella utvecklingen.

Inom samtliga länder med egna procedurer för certifiering har man valt att göra denna funktion myndighetsanknuten. Detta har skett bl.a. med hänsyn till områdets koppling till nationell säkerhet men också mot bakgrund av behovet att kunna ha tillgång till avancerad kompetens. Samtliga myndigheter har en nära koppling till säkerhetsorgan i de aktuella länderna. Senast efter en offentlig utredning har man i Norge valt att lägga denna funktion på Sikkerhetsstaben i Oslo.

I detta sammanhang har Styrelsen för ackreditering och teknisk kontroll, SWEDAC, med hänvisning till lagen om teknisk kontroll (1992:1119), framhållit vikten av att certifieringsfunktionen inte får göras till ett statligt monopol. För kritiska delar av statsförvaltningens verksamhet skulle detta kunna utgöra ett problem, då Sverige som ett litet land knappast har utrymme för mer än en certifieringsfunktion. Inte minst totalförsvaret behöver låta evaluera produkter som har tagits fram för totalförsvarets egna behov, t.ex. kryptosystem. Att därvid helt kommersialisera certifieringsverksamheten, med stark potential av utländskt inflytande, är inte lämpligt. Det är troligt att andra länder kommer att se det som märkligt om vitala behov inom den offentliga sektorn inte möts genom att sektorn själv utövar noggrann tillsyn och kontroll. Därför är det väsentligt att det etableras en certifieringsfunktion i statlig regi.

Problemet ligger till del i att statens egna behov inte enkelt kan lösas genom samverkan mellan myndigheterna (på eget initiativ).³¹ Det är tydligt att den offentliga sektorns behov inte kan lösas utan åtgärder från regeringen. Det torde nu krävas en samordning för att klara ut statens roll och behov. I synnerhet totalförsvaret har kontinuerliga behov av evaluering som dock hittills i huvudsak endast berört speciellt framtagna produkter. I andra fall har evaluering måst utföras utomlands.

³⁰ Statskontorets utvecklingsråd, DAS-90-studien (projekt inom Statskontorets Utvecklingsråd), IT4-projektet Certifiering av IT-Integritet [CITI] 1992, förslag från SAMS och Statskontoret samt SWEDAC

³¹ Efter DAS-90-arbetets avslutande förbereddes i dåvarande Försvarsstaben ett certifieringsråd med deltagande från Statskontoret, Rikspolisstyrelsen och ÖCB. Initiativet föll dock på förvaltningsrättsliga problem som beslutanderätt, överklagande, osv.

Frågan gäller emellertid inte bara den offentliga sektorns egna behov. Exporterande företag inom IT-sektorn måste kunna konkurrera framgångsrikt på den internationella marknaden. Flera företag har efterfrågat möjligheter att låta sina produkter evalueras i Sverige. Många företag känner tveksamhet att överlämna detaljerat konstruktionsunderlag till utländska företag eller tvingas översätta underlag och beskrivningar från svenska. Ett antal företag har uttryckt intresse för att etablera sig som evalueringsföretag.

I IT-propositionen *Åtgärder för att bredda och utveckla användningen av informationsteknik*³² från 1996 talas om behovet av att utveckla "system för certifiering av (IT-säkerhets-) produkter". Sverige bör snarast stödja de internationella ansträngningarna att tillämpa IS 15408 och därvid bygga upp ett sådant system. Statens roll som kravställare, både för egen del, och omsorg om säkerheten i kritiska infrastrukturer inom IT- och kommunikationsområdet talar för att staten aktivt bör verka för att ett system för certifiering av IT-säkerhet i produkter och system kommer till stånd.

7.7.5 Utredningens förslag till certifieringsfunktion för IT-säkerhet i produkter

Som redovisats ovan föreligger i dag en brett tillämpad internationell standard, ISO/IEC IS 15048, för värdering av IT-säkerhet. Standarden kan appliceras på såväl produkter som på enskilda IT-system. Produktevalueringarna dominerar och avser normalt kommersiellt tillgängliga produkter. I vissa fall förekommer det att produkter som inte finns på den öppna marknaden evalueras – det gäller framför allt speciella kommunikationssäkerhetskomponenter som kryptosystem, envägsnätfilter m.m. speciellt utvecklade för statens räkning.

Flera inom försvaret pågående projekt har behov av evaluering av olika produkter, där man hittills i flera fall tvingats söka sig utomlands. Svensk IT-industri har också efterfrågat tillgång till ett svenskt system för evaluering och certifiering. Särbarhets- och säkerhets utredningen föreslår att inom landet byggs upp ett system med en sådan funktion. Härvid erfordras ett svenskt regelverk för hur evaluerings- och certifieringsprocesserna skall realiseras. Det torde vara lämpligt att här bygga på erfarenheter från de länder som sedan ett antal år har etablerat egna system. Vidare

³² Prop. 1995/96:125, bet. 1996/96:TU19, rskr. 1995/96:282

krävs en uppbyggnad av evalueringsföretag som kan utföra det egentliga granskningsarbetet. Ett antal svenska företag har uttryckt intresse för att etableras sig för denna typ av uppgift. SWEDAC bör i detta sammanhang medverka vid ackreditering enligt internationella krav av såväl evalueringsföretag (EN 45001; ISO Guide 25) som certifieringsfunktion (EN 45011; ISO Guide 65).

Till certifieringsfunktionens uppgifter bör höra:

Licensiering av evalueringsföretag efter de principer som tillämpas i andra länder.

Stöd och rådgivning vid utnyttjande av evalueringsstandarden för kravspecifikation.

Tillsyn av evalueringsföretagen vad gäller kompetens och metodik (i samverkan med SWEDAC).

Godkännande av nya evalueringsuppdrag till evalueringsföretagen i syfte att säkerställa en rimlig balans mellan ambitionsnivå (vad gäller assurancesnivå), produktens komplexitet, bedömd erforderlig tid och resursåtgång.

Uppföljning av pågående evalueringsprojekt.

Gransknings av evalueringsrapporter.

Utgivande av certifikat.

Internationell samverkan i syfte att säkerställa och vidmakthålla erkännande av svenska certifikat.

Internationell samverkan i syfte att utveckla effektivare metodik för evaluering.

Lagen om teknisk kontroll (1992:1119) tillkom som ett resultat av en strävan från statsmakterna att avreglera området provning och certifiering. Grunden för ömsesidigt erkännande skall vara internationella standarder och ackreditering via det statliga ackrediteringsorganet, i Sveriges fall SWEDAC. SWEDAC anmäler ackrediterade organ till omvärlden. Ett sådant anmält organ är en av SWEDAC oberoende institution eller motsvarande med uppgift att prova en produkts överensstämmelse med standard och som regeringen har anmält till EG-kommissionen.

Principen att staten inte skall ha ensamrätt inom certifieringsområdet är både riktig och viktig. Dock torde utrymmet för konkurrens för själva certifieringsfunktionen vara begränsat. Som tidigare påpekats torde det vara mindre lämpligt att helt kommersialisera certifieringsverksamheten. Flera länder har låtit sina certifieringsorgan ackrediteras av den nationella ackrediteringsmyndigheten. Samtidigt är tillkomsten av den

internationella överenskommelsen angående erkännande av IT-certifikat ett tecken på en särskild omsorg att säkerställa en jämn och hög nivå på kvaliteten i utfört arbete. Utgångspunkten anges ha varit att endast de aktiva certifieringsorganen har tillräcklig kunskap och kompetens för att utföra den erforderliga kvalificerade granskningen av organen själva (inbördes granskning, *peer review*). Detta kan möjligen ses som en risk för dubbelarbete, men har motiverats, dels av nämnda kompetensskäl, dels med hänsyn till IT-säkerhetsområdets särskilda betydelse för den nationella säkerheten. Till saken hör även att granskningsarbetet i grunden skiljer sig från sedvanlig testning mot överensstämmelse i så motto att man i säkerhetssammanhang strävar efter att skapa underlag och förtroende för icke-existens (av svagheter), snarare än att verifiera viss på förhand definierad funktion.

Tidigare utredningar och projekt har diskuterat hur en certifieringsfunktion kan etableras inom landet. Bland remissvaren på CITI-rapporten³³ föreslog bl.a. Försvarsindustriföreningen att Försvarets Materielverk (FMV) borde få i uppgift att inrätta en sådan funktion.

Det är väsentligt att funktionen har erforderlig kunskap om säkerhetstekniska svagheter och om hur evaluering i praktiken går till. Därför har utredningen funnit att FMV, som sedan slutet av 1980-talet arbetat med evaluerings- och certifieringsfrågor, är lämpat att bygga upp en statlig certifieringsfunktion. Med den kompetens och erfarenhet på området FMV har torde funktionen kunna byggas upp där snabbare än någon annanstans. FMV bör inledningsvis erhålla detta uppdrag med särskilt anslag. Efterhand kan del av certifieringsfunktionen vara självfinansierad via avgifter som tas ut i samband med varje certifiering (t.ex. som en viss andel av evalueringskostnaden). Viss del av funktionens kostnader bör dock även på längre sikt finansieras i särskild ordning. För uppbyggnadsarbetet kan initialt krävas extra resurser.

Ett system för evaluering och certifiering är av vikt också för den allmänna utvecklingen mot bättre IT-säkerhet i samhället. En certifieringsfunktion bör därför i sammanhanget ses som ett stöd inte bara för försvarssektorn utan i väl så hög grad till det civila samhället och dess näringsliv. Detta kan möjligen anses tala mot att ge en försvarsmyndighet som FMV uppgiften. För en sådan lösning talar dock, förutom tidigare nämnda kompetens- och erfarenhetsskäl, även det faktum att FMV redan i dag har uppdrag

³³ IT4-projekt 4112; 1992

inte bara mot Försvarsmakten utan även mot andra delar av totalförsvaret (t.ex. ÖCB). På sikt kan tänkas att FMV uppdrag efterhand breddas när det gäller kvalificerat upphandlingsstöd också utanför totalförsvarssektorn.

Staten har anledning att via berörda myndigheter (exempelvis Statskontoret, Post- och telestyrelsen, Försvarsmakten) utveckla policy för tillit vad gäller upphandling där krav på säkerhet ingår. Man bör här kunna göra jämförelser med regler som tillämpas i t.ex. Storbritannien och USA för produkter som avses ingå i för samhället säkerhetskritiska system.

Sammanfattningsvis föreslår utredningen att FMV får i uppgift att bygga upp ett svenskt system för evaluering och certifiering baserat på IS 15408/EN45001/EN45011.

7.8 Sammanfattning av förslagen

Utredningen har följande förslag inom IT-säkerhetsområdet:

En övergripande strategi för samhällets hantering av IT-säkerhet och skydd mot informationsoperationer.

Ett tvärsektorielt samordningsorgan för IT-säkerhet och skydd mot informationsoperationer inrättas i Regeringskansliet

Att den av utredningen föreslagna planeringsmyndigheten får ett sammanhållande ansvar för samhällets IT-säkerhet.

En funktion för teknikkompetens inom IT-säkerhet, vilken inrättas i FRA-miljö som en egen myndighet med FRA som chefsmyndighet.

En funktion för IT-incidenthantering, vilken inrättas i högskolemiljö som en egen myndighet med PTS som chefsmyndighet.

Att den funktion för omvärldsanalys, vilken inrättas som en del i planeringsmyndigheten, även har kapacitet att bedriva omvärldsanalys inom områdena IT-säkerhet och informationsoperationer.

Att regeringen låter utreda och föreslå författningsändringar för att kunna garantera hög sekretess inom teknikkompetensfunktionen och IT-incidenthanteringsfunktionen samt att medge obligatorisk incidentrapportering för statsförvaltningen.

Att regeringen låter utreda och föreslå författningsändringar för att klargöra förutsättningarna för aktiv IT-kontroll.

Att FMV får i uppgift att bygga upp ett svenskt system för evaluering och certifiering.

Att regeringen undertecknar *Recognition Arrangement for IT Security Certificates*.

8 Civil - militär samverkan

8.1 Bakgrund

I proposition *Det nya försvaret* 1999/2000:30 angavs följande:

”Beträffande uppgiften att stärka det svenska samhället vid svåra påfrestningar i fred skall Försvarmakten ha förmåga att samverka med civila myndigheter och ha förmåga att ställa resurser till förfogande. Försvarmakten skall vidare ha förmågan att ställa resurser till förfogande vid räddningstjänst och därutöver kunna lämna stöd till andra myndigheter. Kraven på förmågan att stärka det svenska samhället vid svåra påfrestningar i fred skall inte utgöra en utgångspunkt för Försvarmaktens utformning men skall beaktas i den operativa och territoriella planeringen, vid planeringen av övningsverksamhet samt när det gäller tillgänglighet till materielslag och förnödenheter.”

En av Försvarmaktens fyra huvuduppgifter är att bidra till att stärka det svenska samhället vid svåra påfrestningar i fred genom att kunna samverka med andra myndigheter och kunna ställa resurser till förfogande. Försvarmakten skall genomföra den planläggning och vidta de förberedelser som behövs för att kunna lösa myndighetens uppgifter. Detta sker nu allt starkare markerat med de senaste försvarsbesluten som grund.

Kravet på förmågan för det militära försvaret att samverka med civila myndigheter tillämpas så att Högkvarteret samverkar med centrala myndigheter och Militärdistriktet samverkar med regionala och lokala myndigheter. Inom Militärdistriktet samverkar i princip staben regionalt och distriktsgrupperna lokalt. Även distriktsgrupperna kan dock samverka regionalt med t.ex. länsstyrelse, länspolis och landsting om samverkan inte kräver omfattande stabsstöd. Inom Militärdistriktets uppgifter ligger att utforma planer för stöd till samhället, även avseende personal- och materielresurser

Även civila myndigheter och organisationer måste enligt utredningen i planering av förberedelser inför allvarliga kriser utveckla organisation och system för att när så är motiverat rekvirera militär insats och att samverka med militära resurser i krishantering. Vid snabba eller osäkra förlopp måste denna förmåga finnas dygnet runt, ibland med kort varsel. Väl inövade system måste finnas för vart civila myndigheter skall vända sig för att få svar på frågor, när kompetensen finns inom Försvarsmakten. Behovet gäller självfallet också hur och var man snabbt kan rekvirera militär medverkan.

Samverkansförmågan måste utvecklas mellan civila och militära myndigheter. Förmågan till samverkan vid svåra kriser eller oklara situationer måste finnas dygnet runt på minst en områdesnivå.

8.2 Erfarenheter av civil-militär samverkan

Erfarenheter av civil-militär samverkan i sen tid finns bl.a. från insatserna med anledning av översvämningarna i Arvika-trakten i Västra Värmland under nov–dec 2000. Militärt stöd begärdes med räddningstjänstlagen som utgångspunkt. Omfattande insatser genomfördes under drygt sex veckor med sammanlagt 14 medverkande militära förband, sex hemvärnsförband samt medverkan av lottakåren. Sammanlagt deltog drygt 100 befäl, ca 1 100 värnpliktiga och 900 hemvärnsmän och lottor. I genomsnitt bestod insatsen av 130 kvinnor och män under perioden, varav 6–8 befäl. Det är angeläget att alla insatser dokumenteras och blir föremål för utvärdering. Så sker också i Arvika-fallet. Insatsen förefaller enligt hittills gjorda iakttagelser och utvärderingar att ha fungerat väl. Det speglar Försvarsmaktens möjligheter och förmåga att medverka under händelser som innebär påfrestningar i det civila samhället.

Vissa initiala problem i insatsen redovisas visserligen i den utvärdering som genomförts av chefen för Mellersta militärdistriktet.¹ Organisationen stämde initialt inte överens med den civila sektorindelningen. ”En ibland kaotisk situation med behov av snabb omfördelning av resurser och sektorchefer och andra befattningshavare som var ovana vid att samarbeta med militära enheter bidrog till den röriga situationen” (sid. 36). De militära reservelverk som skulle tillföras insatsen visade sig förrädsställda

¹ C MD M: Utredning om Försvarsmaktens insatser i Arvika hösten 2000, delrapport 2001-04-25.

på olika håll och vid driftkontroll fungerade de ej. ”Vid provstarter av kompletta elverk fungerade dessa ej på grund av eftersatt underhåll. Onödigt mycket tid åtgick till att transportera delar från olika håll i distriktet och att reparera elverken innan leverans till Arvika” (sid. 49). Dessa exempel gäller dock initiala problem. Som helhet bör de militära insatserna under översvämningarna i Arvika bedömas ha medverkat till ett gott resultat.

Insatsen i Arvika hade ett relativt utdraget förlopp. Under fyra veckor steg vattennivån successivt med drygt tre meter. Det utdragna förloppet gav möjligheter till viss planering, intrimning och korrigerande av insatserna.

I de europeiska översvämningsfall som utredningen låtit en forskargrupp vid FOI studera (bil. 5), redovisas erfarenheter från Frankrike, Nederländerna och Tyskland av mycket kraftigt stigande vattennivåer med höga flöden under relativt kort tid. Ett tänkbart sådant händelseförlopp skulle, liksom ett större dammbrott, ställa större krav på en mycket snabb insatsförmåga, ledning och samband. Såväl ledningsövningar som praktiska övningar mellan civila och militära myndigheter bör regelmässigt genomföras för svåra, komplexa scenarier.

Det är därför angeläget att dra slutsatser av händelseförloppet och insatserna i Arvika anpassade till andra tänkbara förlopp vid framtida översvämningar. Länsstyrelsens åtgärd att utse räddningsledare underlättade i detta fall samverkan med det militära försvaret. Militär distriktsstaben kunde gruppera en samverkansofficer vid länsstyrelsen. En av slutsatserna från översvämningens insatserna i Arvika-trakten är att det kan finnas lägen när det kan vara befogat med författningsstöd för att under klart definierade förutsättningar ha möjlighet att hålla militära resurser i beredskap under icke tjänstetid.

Ytterligare slutsatser är att så snart det står klart att en insats kan komma att pågå under längre tid än några dygn, en vecka eller längre måste en organisation tillskapas med resurser för att kunna bedöma händelseutvecklingen och samordna olika resursinsatser på civil och militär sida som ett led i krishanteringen. Chefen för Mellersta militär distriktet föreslår i sin utvärdering att Högkvarteret, ÖCB och Räddningsverket regelbundet varje år bör genomföra kortare ledningsövningar för att skapa väl fungerande rutiner i rollspelet på olika nivåer vid gemensamma insatser. Den civila målgruppen skulle bl.a. vara räddningstjänstchefer, polischefer samt chefer för katastrofberedskap. Syftet skulle vara att träna ledning och samverkan mellan Försvarsmakten och totalförsvarsmyndig-

heter på central, regional och lokal nivå och härvid testa gällande planer, sambandssystem och datorstödda lednings- och informationssystem. Samtidigt kan scenariemetoder utvecklas.

8.3 Samhällets behov av stöd från Försvarsmakten vid olika kriser

Inom försvarsmakten har tidigare gjorts uppskattningar utifrån försvarsbeslutet 1996 om hur det vidgade säkerhetsbegrepp som inrymmer icke militära hot och risker vid sidan av väpnade anfall skall styra totalförsvarets uppgifter.² De scenarier som bedömts särskilt intressanta gäller främst insatser i samband med:

- Nedfall av radioaktiva ämnen.
- Svåra störningar i elförsörjningen.
- Svåra störningar i telekommunikationerna.
- Svåra störningar i vattenförsörjningen.
- Svåra störningar vid radio och TV.
- Översvämningar och dammbrott.
- Massflykt av asyl- och hjälpsökande.
- Allvarlig smitta.
- Terrorism.
- Kemikalieolyckor och utsläpp av farliga ämnen till sjöss.

Militära insatser i samband med kärnteknisk olycka inom eller utom landet kan vara medverkan i samband med bl.a. indikering av utsläpp, sanering, utrymning/avspärning och sjuktransporter. I samband med svåra störningar i elförsörjningen kan det vara aktuellt med bevakning när sabotagehot föreligger, drivmedelsförsörjning, reservkraft, inkvartering, transporter, vattenförsörjning samt sambands- och ledningsresurser.

Vid svåra störningar i telekommunikationerna kan behov av bl.a. stöd med bevakning och reservkraft samt transporter av personal föreligga. I samband med svåra störningar i vattenförsörjningen kan förutom reservkraft finnas behov av bl.a. vattenrening och vattentransporter till tappningsställen.

Behovet vid översvämningar och dammbrott har belysts i samband med redovisningen av erfarenheter från översvämningarna i Arvika-trakten hösten 2000. Vid extremt snabba förlopp kan också

² C Milo Syd, Försvarsmaktens stöd till det civila samhället vid svåra påfrestningar 1999-06-17.

finnas behov av militär medverkan vid avspärrning, utrymning, trafikreglering, inkvartering, utspisning och krisstöd.

I samband med massflykt av asyl- och hjälpsökande till Sverige kan behov föreligga att i samverkan med bl.a. Migrationsverket och polisen ge stöd med underrättelser om flyktingströmmars riktning och storlek, stöd vid sjöräddning, biträde med dirigering av flyktingtrafiken m.m.

Vid allvarlig smitta kan finnas behov av militära insatser för sjuktransportresurser. Terrorism är att betrakta som grov kriminell handling och därmed en polisiär angelägenhet. Vid militärt stöd måste gränsdragningen mellan polisiärt arbete och militärt stöd vara klar. Militära insatser kan bl.a. bestå av specifik materiel, t.ex. skyddsvästar, hjälmar, mörkerutrustning och förstärkningsvapen, förnödenheter, transporter, utbildning i vapentjänst, ammunitionsröjning och evakuering.

Svåra kemikalieolyckor kan ge allvarliga spridningseffekter över stora avstånd. Militär medverkan kan vara flygtransporter och andra transporter, bistånd med evakuering, utspisning, förläggning samt sanering, avlysning och sjöräddning.

Exemplen på tänkbara militära insatser vid svåra kriser torde i allt väsentligt vara relevanta idag. Insatsmöjligheter bör planeras med avseende på förmåga över tiden till omedelbara eller näst intill omedelbara insatser, inom 24 timmar, 48 timmar eller under längre tid.

Det finns som tidigare redovisats behov av att samöva scenarier över svåra kriser eller händelser mellan militära och civila myndigheter där militärt stöd är motiverat. Särskilt stort är behovet att öva komplexa händelser där flera myndigheter eller aktörer är berörda och där händelseförlopp är snabba, okontrollerade och svårförutsägbara. Metodik bör också övas för att hantera helt oförutsedda svåra kriser eller händelser. Scenarieteknik kan också bidra till att rikta uppmärksamhet på bl.a. gränsdragningsfrågor i civil-militärt samarbete. Det är givetvis en fördel om viktiga principfrågor uppmärksammas i anslutning till övningsverksamhet än att det sker under pågående allvarligt händelseförlopp som kräver stora insatser.

Om polisen exempelvis kunnat använda försvarets helikoptrar i den operativa polisverksamheten för spaning i samband med polis-morden i Malexander hade man höjt sin effektivitet. Flygning fick inte ske till det aktuella spaningsområdet. Polisen tvingades därför transportera spaningsresurser med ordinarie vägfordon. Gällande förordning angavs som skäl för att helikoptrar inte kunde

utnyttjas. Däremot genomfördes vissa transporter av personal med försvarets helikoptrar från Stockholm till Linköping.

Förutsättningarna för militär medverkan i stöd till samhället vid svåra kriser och händelser regleras bl.a. i förordningen (1986:1111) om militär medverkan i civil verksamhet och förordningen (2000:45) med instruktion till Försvarmakten. Det finns enligt utredningen starka skäl att se över gällande regelverk för att klarlägga förutsättningarna för och underlätta civil – militär samverkan vid svåra kriser och händelser. En genomlysning av gällande regelverk sker för närvarande inom ramen för utredningen om översyn av Försvarmaktens stöd till andra myndigheter m.m. (Fö. 2000:06).

8.4 Utnyttjande av militära resurser vid civil krishantering

Som framgått i citat från propositionen Det nya försvaret (prop. 1999/2000:30), skall kraven på den militära förmågan att stärka det svenska samhället vid svåra påfrestningar på samhället i fred inte utgöra en utgångspunkt för Försvarmaktens utformning och omfattning men skall beaktas i den operativa och territoriella planeringen, vid planering av övningsverksamhet samt när det gäller tillgänglighet till vissa materielslag och förnödenheter m.m. Vid militärt och ekonomiskt likvärdiga alternativ skall enligt propositionen den lösning väljas där Försvarmakten bäst kan stödja samhället vid räddningstjänst, vid svåra påfrestningar i fred och vid andra former av stöd till myndigheter

Redan i totalförsvarsbeslutet 1996 betonades vikten av ett helhetstänkande vid utformningen av samhällets åtgärder för att möta olika hot och risker. I beslutet underströks att när resurser dimensioneras med primär utgångspunkt i ett visst hot, bör beaktas möjligheterna och behovet att dra nytta av åtgärderna också inför andra hotsituationer bl.a. för att stärka Försvarmakten förmåga att bistå samhället vid svåra kriser och händelser.

Fördelarna med en helhetssyn när det gäller frågan om avvägning och dimensionering ansågs ligga främst i de samordningsvinster som kan uppnås i utnyttjande av resurserna. Även med beaktande av krav på unika resurser, beredskapskrav eller andra begränsningar i användandet av vissa resurser, bör effektiviserings- och rationaliseringsvinster kunna uppnås genom sam- och

merutnyttjande. Helhetssyn bör således kunna leda till att de totala kostnaderna för samhället att möta hot kan begränsas.

Det framhölls att det ur ett samhällsekonomiskt perspektiv inte är helt godtagbart att resurser som avdelats och dimensionerats för ett visst syfte inte utnyttjas även för andra ändamål när detta är möjligt och ändamålsenligt. Det ger ingen optimal användning av allmänna medel att skapa särskilda resurser för varje form av sällan förekommande stor påfrestning om man med samma resurser kan hantera flera typer av sådana påfrestningar. Härtill kommer att samhällets samlade insatser kan bli mera verkningsfulla om utnyttjande av samhällets alla lämpade resurser ses i ett sammanhang.

De särskilda resurser som avdelas för det militära försvaret bör därför utnyttjas även för att bidra till att förebygga och hantera svåra påfrestningar i fred. Utnyttjande av resurserna får dock inte ske på ett sådant sätt att det inverkar menligt på beredskap och Försvarsmaktens förmåga att lösa sina andra uppgifter.

I totalförsvarsbeslutet 1996 framhölls vidare att den sedan länge i vårt land gällande grundsatsen att militärt tvång eller våld inte skall brukas mot den egna befolkningen eller andra civila utgör en annan självklar begränsning. Militär personal skall således inte ges uppgifter utanför det traditionella militära verksamhetsområdet som rymmer utövning av våld eller tvång mot enskilda. En annan sak är att utnyttja resurser till stöd för andra myndigheter som är lagligen berättigade att använda tvång eller våld. De militära resurserna bör dock i sådana situationer nyttjas på så sätt att det inte kan uppfattas som ett avsteg från de begränsningar som här angetts.

Vidare kan regler rörande konkurrens, upphandling och statsstöd i vissa fall begränsa möjligheterna att utnyttja totalförsvarets resurser för fredstida ändamål.

Av beslutet 1996 framgick också att utnyttjande av militära resurser vid svåra kriser eller händelser kan ske i form av bistånd vid akuta påfrestningar, då samhällets resurser i övrigt är otillräckliga och behöver kompletteras. Det gäller särskilt vid svåra kriser med snabba och oförutsägbara förlopp. Ett mera regelbundet och planerat utnyttjande kan i vissa fall också vara motiverat. Även integrerade resurser, dvs. resurser som dimensioneras och utnyttjas för uppgifter i såväl fred som vid höjd beredskap kan övervägas. Regelbundet utnyttjade och integrerade resurser bör i så fall regleras i särskild ordning i berörda myndigheters instruktioner och inom ramen för budgetprocessen.

8.5 Samutnyttjande av resurser på Gotland

Utredningen fick den 7 december 2000 ett tilläggsdirektiv av regeringen för att nära följa det arbete som bedrivs av Rikspolisstyrelsen, Försvarmakten, Kustbevakningen, Tullverket, Länsstyrelsen i Gotlands län och Sjöfartsverket i enlighet med regeringens beslut den 20 juli 2000 om att belysa behovet av och möjligheterna att utnyttja sina resurser gemensamt. Vid behov skulle också övervägas hur myndigheternas erfarenheter skulle kunna användas för att åstadkomma en förbättrad helhetssyn.

Bakgrunden är att regeringen i propositionen *Det nya försvaret* (prop. 1999/2000:30) angav att frågan om att utnyttja militära resurser till stöd för andra myndigheter borde bli föremål för en mera generell översyn. Som ett led i en sådan översyn kunde det vara värdefullt med en regional försöksverksamhet för att belysa möjligheterna till ytterligare samverkan mellan Försvarmakten och civila myndigheter. Riksdagen gav som sin mening tillkänna att Gotland görs till försöksområde för samordning av militär och civil krishantering.

Sårbarhets- och säkerhetsutredningen har därefter deltagit i den arbetsgrupp som bildats. Arbetet har slutförts i enlighet med uppdraget. En redovisning av regeringens uppdrag rörande allvarliga olyckor och särskilda samhälleliga kristillstånd har under april 2000 överlämnats till försvarsministern.

Som en bakgrund redovisas Gotlands förutsättningar, generellt och inom viktiga samhällsområden. Därefter har en översiktlig analys gjorts av behov av och möjligheter till samutnyttjande av resurser på och runt Gotland. Några modeller för krishantering innebärande ökat samutnyttjande av resurser har studerats och jämförts med dagens situation. Slutsatserna härifrån har legat till grund för överväganden om förändringar i bl.a. organisation och ledningsstruktur samt förslag om ett samverkanscentrum och en försöksverksamhet på Gotland.

8.5.1 Befintlig organisation och ledningsstruktur

Inom vissa områden har myndigheterna var för sig resurser och verksamhet som skulle kunna samutnyttjas respektive samordnas. Här kan exempelvis nämnas ledningscentraler, patrullverksamhet samt stödresurser som förråd och verkstad. Det finns även unika resurser, vars närvaro på ön kan vara av livsavgörande betydelse.

Bland dessa kan nämnas helikoptrar, sjuktransportfordon, tryckkammare och miljöskyddsfartyg med räddningsdykargrupp.

Myndigheterna har idag olika regionindelningar, optimerade ur respektive myndighets uppdrag och inte ur Gotlands perspektiv. En samverkande regional ledning för att i ökad utsträckning kunna samutnyttja resurserna på och runt Gotland, samt ökade möjligheter att utnyttja Försvarsmaktens resurser, torde öka förutsättningarna för ett effektivt och ekonomiskt utnyttjande av resurserna.

8.5.2 Behov av och möjligheter till samutnyttjande av resurser

Exempel på allvarliga olyckor och särskilda samhälleliga kristillstånd är enligt redovisningen:

- Nedfall av radioaktiva ämnen över Gotland.

- Svåra störningar i viktiga infrastruktursystem: el-, tele-, data-, vatten- och informationsförsörjning.

- Angrepp på infrastruktur från okänd aktör.

- Fartygsolyckor och olje- och kemikalieutsläpp (sjöräddning eller miljöräddningstjänst till sjöss).

- Flygolyckor.

- Olje- och kemikalieolyckor på land.

- Massflykt av asyl- och hjälpsökande till Gotland.

- Allvarlig smitta.

- Terrorism.

- Påfrestningar orsakade av svåra väderförhållanden.

- Omfattande bränder.

Beredskapen inför krissituationer på Gotland måste dock vara sådan att den kan möta varje hot, även de som inte har förutsetts.

Samverkan är en nödvändig förutsättning för en effektiv krishantering. Hit hör främst:

- Att snabbt få tillgång till en korrekt lägesbild är av avgörande betydelse i alla krissituationer.

- Ledningsfrågan är central. Det handlar både om behovet av att en effektiv, samgrupperad och samverkande ledning snabbt kan byggas upp, och om att under långvariga insatser har tillräcklig ut hållighet. I ledningen ingår också att ha tillgång till stabsresurser och tekniska stödsystem.

- Information, samordnad, korrekt och snabb, är av grundläggande betydelse och kräver långtgående samverkan och teknikstöd.

Speciellt viktigt är att informationsfunktionen omedelbart kan börja verka.

Fungerande transporter är en förutsättning för tillförsel av resurser från fastlandet och av transport av skadade m.fl. i andra riktningen. Också som ett led i en insats kan transportresurser vara nödvändiga. Helikoptrar är här av speciellt intresse, och det är viktigt att de är snabbt tillgängliga.

Sjukvårdsresurserna på Gotland är begränsade, något som i sin tur ställer transportfrågan i fokus, både för att få dit sjukvårdspersonal och för att kunna transportera svårt skadade till fastlandet. Här handlar det om att snabbt aktivera de reservmöjligheter som finns på ön (ambulanser, frivilliga).

8.5.3 Förändring av organisations- och ledningsstruktur

Arbetsgruppens enhälliga slutsats har blivit att till regeringen lägga förslag om att inrätta ett samverkanscentrum, kallat GotSam. Med ett permanent bemannat, samgrupperat samverkanscentrum skulle kraven på snabbt igångsättande av ledning tillgodoses. Detta centrum bör innefatta lokal och utrustning för ledning i samverkan av vissa funktioner såväl under normala förhållande som vid allvarliga olyckor och särskilda samhällsliga kristillstånd på och runt Gotland.

Initialt medför förslaget vissa kostnader för iordningställande av lokal med teknisk utrustning, flyttkostnader m.m. Mer påtagliga ekonomiska vinster bedöms kunna tillgodoräknas först när verksamheten nått en viss omfattning. Här kan besparingar nås i gemensam administration och andra stödfunktioner, samtidigt som dagliga kontakter och gemensam utbildning skulle möjliggöra en mer flexibel användning av personalresurserna.

Både effektivitets- och kvalitetsmässiga vinster kan väntas uppnås genom en samgruppering. Dessa vinster handlar bl.a. om samverkan i beredskap, snabbt igångsättande av insatser och smidig tillgång till resurser, samordnad information, möjligheter till samplanering och gemensam utbildning samt ökad uthållighet och flexibilitet.

8.5.4 Syftet med en försöksverksamhet

Myndigheterna och Gotlands kommun föreslår att en försöksverksamhet genomförs, där bl.a. möjligheterna till ytterligare samverkan med Försvarmakten och civila myndigheter kan belysas. Försöksverksamheten bör omfatta samgruppering av vissa myndigheter kring samordnad omvärlds- och resurslägesinformation, planering och beredskap.

Syftet med försöksverksamheten bör vara att:

- Pröva samgruppering.
- Pröva en samgrupperad och samverkande regional ledning vid övningar av en rad scenarier.
- Utvärdera nyttan av samgruppering, främst med avseende på olika krisledningskomponenter.
- Pröva möjligheterna till ett kostnadseffektivt samutnyttjande av resurser.
- Ge underlag för beslut om framtida samverkansmodell.

Försöksverksamheten bör också enligt arbetsgruppen omfatta fortsatta försök på Gotland med radiokommunikationssystem enligt TETRA-standard, och utveckling av ett övergripande krisdatabas som knyter ihop olika ledningssystem.

Samverkan i civil och militär krishantering är en väsentlig del i försöksverksamheten. Sårbarhets- och säkerhetsutredningen har deltagit i arbetsgruppen och står bakom de slutsatser och förslag som redovisats till regeringen. Utredningen anser att ett genomförande av försöksverksamheten bör kunna ge ett värdefullt underlag för att utveckla civil-militär samverkan, främst med avseende på krishantering. Samtidigt kan en försöksverksamhet ge underlag för bedömningar av möjliga effektivitetsvinster och kostnadsbesparingar samt för behov av att utveckla gemensamma eller integrerbara ledningssystem.

8.6 Militär medverkan i humanitära biståndsinsatser

Såväl den Europeiska unionen som Förenta Nationerna utvecklar formerna för internationell krishantering. Den omfattande del som ryms inom begreppet fredsfrämjande insatser eller motsvarande behandlas inte av utredningen.

Antalet naturkatastrofer i världen har ökat under det senaste decenniet. Det har också på ett markant sätt ökat behovet av såväl

internationella hjälpinsatser som av samordning av hjälpinsatserna. Jordbävningen i Turkiet, orkanen Mitch i Centralamerika samt översvämningarna i Limpopofloden och Zambesifloden i Mocambique är exempel på naturkatastrofer som krävt stora internationella hjälpinsatser och där behovet av koordinering av insatserna varit mycket stora.

I civila insatser i samband med internationella katastrofer, jordbävningar översvämningar eller andra allvarliga olyckstillstånd, finns ofta behov av militär kompetens och militära insatser, i princip under civil ledning. Det gäller även av andra humanitära biståndsinsatser, t.ex. av min- och ammunitionsröjning på land och till sjöss.

Sverige bidrar som biståndsgivare med omfattande stöd till humanitära biståndsinsatser, inte minst för min- och ammunitionsröjning. Svensk militär kompetens tas endast i begränsad omfattning till vara vid insatserna. Däremot förekommer att andra länder hyr in eller anställer svenska militärer för insatser inom t.ex. min- och ammunitionsröjning.

Biståndsinsatser motiveras av humanitära skäl. Det är en självklar princip som inte ifrågasätts av utredningen. Däremot konstaterar utredningen att det vore önskvärt med en ökad medverkan i internationella humanitära biståndsinsatser av såväl civil som militär kompetens. Erfarenheter av tidigare och pågående svenska insatser är goda. Ett ökat engagemang och deltagande i internationella humanitära insatser skulle dessutom bidra till kompetensutveckling för krishantering i svåra, oväntade miljöer och situationer.

Det är enligt utredningen önskvärt att den svenska krishanteringsförmågan utvecklas så att den kan vara en resurs också vid internationella katastrofer och vid humanitära biståndsinsatser, såväl i ett europeiskt som i ett FN-perspektiv.

8.7 Sammanfattning och förslag

Utredningen har i detta kapitel behandlat olika frågor om samverkan mellan det militära försvaret och det civila samhället vid allvarliga kriser i fredstid. Den genomgång som utredningen har gjort visar att det finns goda möjligheter att genom en sådan samverkan nå större effektivitet i utnyttjandet av samhällets samlade resurser för att hantera allvarliga krissituationer. Erfarenheten från olika krissituationer visar att det militära försvaret kan bidra med värde-

fulla insatser och att samverkanspotentialen ännu inte är fullt utnyttjad.

Utredningen anser att vissa åtgärder bör vidtas för att utveckla samarbetet:

1. En inventering av de författningsmässiga hinder som kan finnas mot en fördjupad civil-militär samverkan bör göras. Därefter bör de författningar som utan anledning lägger hinder i vägen ändras.
2. Det är väsentligt att ge civila myndigheter en bättre överblick över vilka möjligheter och begränsningar som det militära försvaret har att stödja det civila samhället vid allvarliga krissituationer i fred.
3. Gotlandsförsöket är ett exempel på att särskilda organisationsformer i vissa fall kan utveckla samarbetet. Förutsättningar kan finnas för lokala eller regionala insatser av detta slag också på andra håll.
4. Utredningen anser att det finns anledning till ett mera omfattande, utvecklat samarbete mellan militära och civila myndigheter också vid humanitära insatser under civil ledning utomlands.

9 Långsiktiga sårbarhetsfaktorer - klimat och bioteknik

9.1 Bakgrund

Samhällets system för säkerhet och beredskap måste innefatta förmågan att följa utvecklingstrender som har eller kan få betydelse för framtida inriktning och utformning av säkerhetsarbetet. Långsiktigt verkande faktorer som klimatutvecklingen och den biotekniska utvecklingen måste av denna anledning tillmätas stor betydelse. Forsknings- och utvecklingsarbete inom dessa sektorer kräver tvärssektoriell samverkan.

Utredningen har tillsammans med Naturvårdsverkets avdelning för miljöanalys genomfört ett tvärvetenskapligt seminarium/workshop för att kartlägga och belysa nuvarande kunskapsläge vad gäller sårbarhet och effekter av klimatförändringar. Redovisningarna har delvis utgått från resultat från SWECLIM-projektet, ett forskningsprojekt finansierat av Stiftelsen för Miljöstrategisk forskning, MISTRA, och Sveriges Meteorologiska och hydrologiska institut, SMHI, med bl.a. Naturvårdsverket som intressent.

De slutsatser som redovisas i det följande med avseende på klimatutvecklingen bygger i huvudsak på de många och i väsentliga delar samstämmiga rön som redovisades under seminariet.

I flera globala klimatstudier anges en temperaturhöjning med 2,5 grader C under de kommande 50–100 åren som sannolik. En global ökning av temperaturen med 2,5 grader C bedöms ge en ökning i Sverige med ca 4 grader C som årsmedelvärde, med en större ökning på vintern än på sommaren. Tillsammans med en förväntad ökad årsnederbörd med ca 10–20 procent medför det effekter i alla naturmiljöer och i samhällets olika sektorer. Överfört till klimatzoners förflyttning motsvarar detta en förflyttning på 0,5 till 1 meter i timmen. För närvarande finns inte bedömningar av hur stormfrekvens och extremnederbörd kan förändras i framtiden.

En del av dessa klimateffekter leder till en förändrad känslighet. Antalet dagar med extrem kyla bedöms minska, vilket minskar riskerna för köldskador av olika slag. Andra effekter på klimatet kan ge en ökad känslighet och sårbarhet, särskilt i fjällekosystem och i Östersjöns känsliga brackvattenkosystem. Även hastigheten i klimatförändringarna kan ge en sårbarhet i ekosystem med lång omloppstid, som skog.

Samhällets känslighet för klimatförändringar är stor inom flera viktiga områden, som säkra transporter, säker elförsörjning, dammsäkerhet och människors hälsa. En framtida sårbarhet beror till stor del på hur vi idag planerar och tar hänsyn till dessa förändringar genom olika anpassningar och genom att öka säkerhetsmarginalerna, där stor risk finns. Det senare gäller särskilt om extrema vädersituationer med stormar och extremnederbörd blir vanligare.

9.2 Kunskapsläget

Redan nuvarande klimat och väder kan ge stora effekter och sårbarhet i svensk naturmiljö och samhällets olika delar, främst teknisk infrastruktur. Särskilt svåra påfrestningar och skador uppstår vid starka stormar – ofta i komplexa kombinationer av olika effekter (t.ex. storm och högt vattenstånd).

En global uppvärmning har observerats under 1900-talet. Förklaringen till utvecklingen under de senaste 30 åren är utsläpp av växthusgaser. Effekterna har också kunnat ses i t.ex. glaciärernas mäktighet och havsisens utbredning.

Både temperaturen och nederbörden har ökat i Sverige under de senaste 140 åren. Sett mer i detalj har det dock förekommit både upp- och nedgångar. För temperaturen är uppgången tydligast under våren. För ökningen av nederbörden bidrar alla årstider utom sommaren, som inte visar någon klar trend. När det gäller extrema väderhändelser (köld, hetta, stor dygnsnederbörd, stormar) kan man möjligen se en tendens till fler värmerekord och färre köldrekord under de senaste decennierna, medan det i övrigt är svårt att se några varaktiga förändringar.

Teknisk infrastruktur uppförs och anläggs ibland utan att tillräcklig hänsyn tas till väderhändelser (extremvindar och extrem nederbörd) som inträffar mycket sällan med nuvarande klimat. Långa klimatologiska mätserier bör återanalyseras för att ge en

bättre grund för känslighet och sårbarhet i såväl nuvarande som framtida klimat.

Klimatförändringar kommer att inträffa i Sverige – förr eller senare och påverkar såväl temperatur som nederbörd. Utgångspunkten för sårbarhetsanalysen är SWECLIM:s klimatscenarier, som är relevanta för förändrat klimat på 50 till 100 års sikt.

Det nordiska klimatet har en större känslighet än det globala i genomsnitt. Årstiderna förskjuts och vi kan få en betydligt kortare vintersäsong. Östersjöns ytvattentemperatur bedöms öka med 2–3 grader C.

Extremvärden för temperaturer påverkas också. Extremt höga temperaturer höjs lika mycket som ökningen av medeltemperaturen under sommaren. Extremt låga temperaturer höjs betydligt mer än ökningen av medeltemperaturen under vintern.

Den hydrologiska cykeln blir mer intensiv. Nederbörden och vattentillgången ökar i stora delar av landet med 10–20 % som årsmedelvärde, mer under hösten. En ökad medeltemperatur ger en ökad avdunstning från mark och vatten. Vissa delar av södra Sverige kan då få vattenunderskott och torra, speciellt under sommaren.

En viss ökning av medelvinden kan ses över landet och särskilt på stora insjöar och på vissa havsområden. Nuvarande modellberäkningar kan inte ge grund för en bedömning av förändrad stormfrekvens.

Effekter och sårbarhet beror såväl på klimatförändringar som på andra faktorer. Viktiga andra faktorer för att bedöma sårbarheten kan vara:

Utveckling av infrastruktur, särskilt teknisk infrastruktur med lång livslängd, såsom vägar, broar, vattenvägar, byggnader, industrier, hamnar, kraftledningar och dammar.

Befolkningsdynamiken sett över 50–100 år och dess effekter på samhällsekonomi och fördelning av samhällets disponibla resurser.

Andra miljöproblem som ändras över tiden, t.ex. tillförsel av näringsämnen till vatten och mark, spridning av miljögifter samt utnyttjande av ändliga och förnyelsebara naturresurser.

Effekter och sårbarhet i naturmiljö, samt jord- och skogsbruk:

Effekterna blir påtagliga för hydrologiska förlopp. Ett förändrat klimat med ökad nederbörd och temperatur enligt SWECLIM:s scenarier ger högre vattenföring i landets norra delar, men mer

variabla förhållanden i södra Sverige. Allmänt påverkas också den säsongsvisa fördelningen, med mer vattenföring under vintern och en tidigare men mindre kraftig vårflod i förhållande till nuläget. Jämfört med dagens klimat kan vattenföringen bli mer extrem under hösten.

Högre vattenflöden i vattendragen och högre nivåer i sjöar och vattendrag påverkar strändernas fysik och ekologi. En reglering av flöden och vattennivåer kan till del motverka de negativa effekterna av högt flöde och höga nivåer.

Snötäcket bedöms bli mindre utbrett och ligga kvar kortare tid. Södra Sverige kommer i medeltal inte att ha vintersnö som ligger kvar. Östersjöisen kommer att bli mindre utbredd och i medeltal endast förekomma i Bottenviken och i delar av Bottenhavet. Det förändrade snötäcket kombinerat med förändrade vintertemperaturer har stor betydelse för tjäldjupet. På snöfria ytor minskar tjäldjupet med högre temperaturer. På snötäckta ytor kan uppvärmningens effekt motverkas av mindre isolering då snödjupet minskar.

Ett förändrat klimat enligt SWECLIM:s scenario bedöms ge ökad tillväxt i skogsbruket och jordbruket (både nya grödor och ökad tillväxt). En viss ökad känslighet och sårbarhet finns genom att många skadedjur och sjukdomar idag hålls nere genom våra klimatförhållanden.

Det finns stora potentiella effekter på Östersjön som ekosystem. En förändrad temperatur påverkar direkt olika arter, liksom förändrade isförhållanden. En ökad nederbörd i tillrinningsområdet till Östersjön bedöms tillföra mer vatten, vilket kan – om inte det motsvaras av en ökad frekvens saltvatteninbrott - leda till en avsevärd utsötning av vattnet. En ökad vattenföring till Östersjön bedöms också tillföra mer näringsämnen, särskilt om nederbörden sker på hösten. Effekterna av dessa förändringar skulle kunna förtränga marina arter (torsk) till fördel för limniska arter (abborre, gädda, gös). Risker finns att främmande arter kan spridas till Östersjön. Dynamiken för algbloomning i Östersjön kan också påverkas.

Våtmarker spelar en viktig roll i kolets globala kretslopp och utgör en stor andel av Sveriges yta. Deras framtida roll i det globala kretsloppet beror ytterst på den hydrologiska statusen i våtmarkerna. För stora delar av Sverige kan våtmarkerna fortsätta ta upp koldioxid från atmosfären. Effekterna på biologisk mångfald i våtmarkerna av en klimatförändring är lite kända.

Plötsliga förändringar och överraskningar kan inte uteslutas, vilket visar på behovet av ett säkerhetstänkande för att bevara ekosystem och biologisk mångfald.

9.3 Effekter på sårbarhet, infrastruktur och hälsa

Risken för erosion, skred och ras ökar med intensivare hydrologiska förlopp och kan hota infrastruktur som vägar, banvallar, broar, byggnader, dammar, avlopps- och vattenförsörjningssystem.

Samhället behöver en god förmåga att ingripa vid akuta händelser för att minska konsekvenserna vid framtida extrema väderhändelser. Stark vind, storm och orkan, extrema mängder nederbörd, snö och isbeläggning samt saltbeläggning är de faktorer som ger störst skada på infrastruktur. Vid dessa extrema väderhändelser drabbas ofta stora regioner och med flera effekter samtidigt.

Särskilt svåra konsekvenser uppstår vid störningar i elförsörjningen eftersom samhällets andra delar är beroende av säker eltillgång. Till andra delar av samhället räknas, transporter, IT-system, telesystem, vatten- och avloppssystem, industrier etc. För eldistributionen finns de av väderhändelser känsligaste delarna i de regionala och lokala näten, särskilt i de fall då områden försörjs via luftledningar i skogsområden. Till del kan känsligheten och sårbarheten minskas genom ett strategiskt uppbyggande av ökad säkerhet i elförsörjningen och elreservkapacitet.

En ökad temperatur i våra sjöar kan ha stora effekter på kvaliteten för dricksvatten, såväl smak, lukt och färg. Det finns en ökad risk för smittämnes- och giftspridning om översvämningar uppströms för ut föroreningar i sjöar och vattendrag som används som dricksvattentäkt. Infrastrukturen för vattenförsörjningen har mycket lång livslängd men är känslig för ett förändrat klimat: en långsiktig strategi för minskad sårbarhet måste därför säkra alternativa vattentäkter, särskilt grundvattenmagasin. Södra och sydöstra delen av landet är här särskilt känsliga.

Ett förändrat klimat med mildare vintrar och förlängda vår- och höstsäsonger kan öka smittspridningen av sjukdomar. Smittämnesbärare som råttor, vissa insekter och fästingar gynnas av ett mildare klimat, vilket ökar risken för spridning av sjukdomar som TBE (fästingburen hjärninflammation), borrelia, vissa diarrésjukdomar och myggburna infektioner. Ökade temperaturer kan också öka risken för dricksvatteninfektioner. Pollenallergier och astma för-

väntas få ändrat säsongsinjuktande, möjligen även en ökning av anfallsintensiteten. Den lägre frekvensen av extrem kyla kommer att ge färre köldrelaterade sjukdomar och skador.

Effekterna av klimatförändringar i vår omvärld kan leda till förändrade förutsättningar och där minska möjligheterna för ett ut hålligt jord- och skogsbruk. Detta kan då leda till en ökad mängd klimatflyktingar. Riskerna för storregionala konflikter i vårt när-område kan inte uteslutas.

9.4 Forsknings och utvecklingsbehovet

Utvecklingen av modeller måste fortsätta och klimatscenarier tas fram för att studera extremer i förhållande till förändringar i medelvärden. Det behövs förbättrad kunskap om hur de storskaliga beräkningsresultaten simulerade med globala modeller ska tolkas vidare till regional skala. Vidare behövs förbättrad integration (t.ex. återkopplingar) mellan olika modeller som beskriver meteorologi, hydrologi, oceanografi och ekosystem.

Genom studier av långa tidsserier (30 år eller mera) kan man fånga upp situationer som har låg frekvens och därigenom göra bedömningar av extrema situationer. Det behövs även studier för att ge bättre kvantitativa bedömningar av felkällor och osäkerheter.

Forskning är nödvändig för att ge underlag för effektstudier inom andra områden och sektorer (jordbruk, skogsbruk, ekosystem, samhällstruktur, kustzoner) Effektstudier bör utvecklas för samtliga sektorer som är känsliga för klimatpåverkan:

Jord- och skogsbruk, fiskerinäring, rennäring.

Hydrologiska förlopp, mark och grundvattenförhållanden och deras betydelse för skred, ras och erosion.

Limniska, marina och terrestra ekosystem, med hänsyn taget till andra faktorer som påverkar dessa miljöer.

Sverige har en unik position för att studera sjukdomars utbredning i en klimatgradient. Dessa studier kan vara en viktig länk i att bedöma framtida globala hälsoeffekter av klimatförändringar.

Anpassning till ett förändrat klimat:

Grundläggande kunskaper om dynamiska förlopp i nationella, regionala och lokala ekosystem.

Hur vi idag kan ta hänsyn till kommande förändrade villkor för samhällets byggnation av infrastruktur (bl.a. vägar, broar, vatten- och avloppssystem, dammar, etc.) med lång livslängd. Till del finns kunskaper om klimatets betydelse för infrastrukturen. Dessa kunskaper bör kunna utnyttjas på ett mer konsekvent sätt i riskbedömningen vid investeringar i infrastruktur.

Hur naturvärden (fjäll, skogs- och jordbrukslandskap, kustzoner) och biologisk mångfald kan bevaras genom skapande och säkerställande av migrationskorridorer och av mikromiljöer, som ökar robustheten vid klimatförändringar.

En anpassning till ett förändrat klimat kräver nya kompetenser i samhället, nytt underlag för beslut och nya arenor för politiska beslut.

Inom MISTRA övervägs nu enligt vad utredningen erfarit att göra ytterligare satsningar inom området. Det är angeläget att så kan ske och att resultaten tillgodogörs i åtgärder för att minska samhällets sårbarhet.

9.5 Bioteknisk utveckling

Utredningen har inte haft samma möjligheter som vad gäller klimatfrågorna att studera och värdera den biotekniska utvecklingen i ett sårbarhetsperspektiv. Det är dock en angelägen uppgift.

Den biotekniska utvecklingen medför både naturliga mutationer i virus och andra mikroorganismer och, som en följd av en helt ny avancerad teknologi, avancerade möjligheter att gentekniskt förändra växters, djurs och människors egenskaper. Utvecklingen inrymmer i sig stora möjligheter men också en betydande sårbarhet. Kartläggningen av den genetiska koden kan tillsammans med andra biotekniska landvinningar ge påverkansmöjligheter som medför risker om de används ovarsamt, i samband med hot eller på annat sätt i skadeframkallande syfte.

De flesta länder eftersträvar att etablera en industriell infrastruktur för bioteknik. Utvecklingen inom biotekniken kommer att vara mycket snabb och inrymma nya hot. Den inrymmer också risker för en ökad frekvens genetiskt utvecklade stridsmedel i strid med internationella regelverk och en spridning av dessa till aktörer som inte behöver vara stater. Den snabba utvecklingen inom

bioteknikområdet är samtidigt ett starkt motiv för att studera och analysera de långsiktiga effekterna.

Samhällets sårbarhets- och säkerhetsarbete måste inrymma även dessa perspektiv både i planering och i insatser för forskning och utveckling. Såväl klimatutveckling som bioteknisk utveckling förutsätter aktiv medverkan i internationellt arbete.

10 Forskning för civilt försvar och krishantering

Den svenska försvarssektorn har traditionellt satsat betydande resurser på forskning och studier. Denna investering har ansetts nödvändig för att säkerställa ett kunskaps- och teknikunderlag för försvarets operativa förmågor. Det militära försvaret har därvidlag prioriterats resursmässigt i linje med den hotbild och de kapacitetsbehov som funnits under större delen av efterkrigstiden. Även inom det civila försvaret har betydelsen av forskning och studier lyfts fram, särskilt under den senaste tioårsperioden. Det finns ingen anledning att nu bryta denna tradition av investeringar i långsiktigt kompetenshöjande och kunskapsuppbyggande verksamheter inom totalförsvarsområdet.

Efter hand har en breddad hotbild och ett nytt säkerhetspolitiskt koncept vuxit fram. Försvaret fick genom riksdagens beslut 1996 fyra centrala uppgifter, varav två var nya. Särskilt den fjärde uppgiften att stärka det svenska samhället vid svåra påfrestningar i fred berör det civila försvaret, men även internationella insatser (den tredje, att bidra till fred och säkerhet i omvärlden) engagerar detta område. Sedan 1996 års ominriktningsbeslut har betydelsen av militär och civil samverkan, bland annat inom krishanteringsområdet, ytterligare befasts. Det svenska åtagandet att bidra till EU:s militära och civila krishanteringskapacitet ställer ytterligare krav på kompetens och förmåga.

För den fjärde uppgiften framstår de nationella ledningsfrågorna i bred bemärkelse som centrala. Detta nya ansvar innebär radikalt annorlunda problemställningar för det civila försvaret än tidigare fokusering på att erbjuda stöd till Försvarsmakten vid ett väpnat angrepp eller vid nationell isolering. Nu gäller i vissa avseenden den omvända situationen, dvs. det militära försvaret förväntas ge stöd till samhället vid civila, men potentiellt konfliktfyllda, svåra händelser inom eller utanför landet. Den ursprungliga totalförsvarstanken byggde främst på principen om samhälleligt

stöd till nödvändiga militära insatser till skydd av landets territorium och nationens överlevnad.

Inte alla säkerhetspolitiska utmaningar kan lösas med militära medel. En rad civila resurser och förmågor måste mobiliseras för att skydda samhällets vitala funktioner i olika avseenden. Ett exempel är säkrandet av rikets ledning vid en svår nationell påfrestning. En sådan förmåga ställer en rad krav på fungerande informations-teknologi, en acceptabel informationshantering samt en fungerande kapacitet för beslut, implementering och styrning. Endast i begränsad utsträckning kan den militära infrastrukturen och dess specialkompetenser stötta den nödvändiga civila ledningskapaciteten.

Krishantering kräver, som visats i tidigare avsnitt, förmåga inom många områden. Det gäller skydd av infrastruktur, nationell, regional och lokal samordning och ledning, hantering av akuta och konsekvensskapande händelser, förmåga att kunna lämna psykologiskt och andligt stöd samt ett utbrett medborgerligt förtroende och engagemang för demokratin och rättsstaten. Därtill krävs ett internationellt arbete för att säkerställa denna förmåga i Europa och i FN-sammanhang.

10.1 Resurser för nya uppgifter

Med den ominriktning av det svenska totalförsvaret som skett genom de senaste försvarsbesluten är det rimligt att även en viss omDispositioner sker av den forsknings- och studieverksamhet som bedrivs för att bygga upp nödvändig förmåga och kompetens både för det civila försvarets behov och för att utveckla samhällets förmåga att såväl förebygga, skapa beredskap inför, hantera och utvärdera kriser.

Dagens resursprioriteringar inom forskningsfältet speglar tidigare epokers behov och motsvarar inte helt de målbilder som nu lyfts fram i försvarsplaneringen. Inte minst är det ämnesmässigt breda och komplexa civila försvarets forskningsinsatser blygsamma jämfört med resurserna för teknikutvecklande och kompetenshöjande militär forskning. Den tredje och fjärde uppgiften har ännu inte fått ett resursmässigt genomslag inom försvarsforskningen trots att uppgifterna i hög grad berör det civila försvaret nationellt och internationellt.

Ett framtida ställningstagande i den centrala resursprioriteringsfrågan bör av dessa skäl enligt utredningen även inrymma ett ställ-

ningstagande för en ökad forskning för civilt försvar och krishanteringsförmåga. Stora krav måste ställas på planering, uppföljning och utvärdering av forskningen. Det bör vara den föreslagna nya planeringsmyndighetens och inte minst regeringskansliets ansvar att säkerställa att FoU-insatserna inom den civila delen inriktas mot relevanta frågeställningar, som samordningsförmåga, ledningsförmåga, anpassningsförmåga och operativ krishanteringsförmåga.

Forskningen inom krishanteringsområdet befinner sig i ett utvecklingsskede och kan ge väsentliga bidrag till samhällets möjligheter att förebygga och begränsa skadeverkningarna av allvarliga kriser. Den nya planeringsmyndigheten som beskrivs i kapitel 5 bör därför också ha egna medel för forsknings- och utvecklingsändamål inom krishanteringsområdet. Myndigheten kan då uppträda som beställare av forskning och utveckling av förmåga inom detta område.

En viktig aspekt är också hur forskare kan stimuleras att bidra till denna nödvändiga kunskapsuppbyggnad. Det är inte självklart att dugliga forskare inom till exempel det samhällsvetenskapliga området finner förutsättningarna tillräckligt goda för att inrikta sin energi på dessa angelägna frågor. Övergripande styrning och uppföljning är endast en del av problematiken. Incitamentsstrukturer behöver skapas för att engagera landets forskarbegåvningar inom detta område.

10.2 Forskning till stöd för utbildning

Även kompetensförsörjningen behöver förändras. Utbildningen av personal inom sårbarhets- och säkerhetsområdet måste i högre grad än som nu är fallet styras mot de arbetsuppgifter som kan anses vara centrala för befattningshavare under deras yrkesverksamma tid. Utbildningen måste förbereda inför kommande uppgifter och kan inte läggas upp efter tidigare epokers hotbild och yrkesbehov. En betydande omdaning av utbildningsformerna och kursinnehållet inom totalförsvarets område torde vara en nödvändig förutsättning för att engagera unga människor i detta arbete. Försvarsområdet konkurrerar med andra tjänstesektorer om det begränsade tillflödet av välutbildade och arbetssugna ungdomar.

Vid Försvarshögskolan bedrivs ett viktigt utvecklingsarbete i denna riktning. FHS genomför, förutom utbildningen av officerare, en rad program och enstaka kurser för civila inom total-

försvaret samt för universitetsstuderande med inriktning mot en yrkesframtid inom området. Chefskurser i internatform har erbjudits sedan 1950-talet. Utbildningen akademiseras och är i flera avseenden likvärdig med annan svensk högskoleutbildning. Skolans program och utbildningsprofil internationaliseras för att dess forskning skall kunna bli en givande part i det internationella kunskapsutbytet.

Liksom är fallet inom högskolan i övrigt, måste kopplingen mellan utbildning och forskning stärkas. Utbildningen skall vila på vetenskaplig grund, liksom på beprövad erfarenhet. Ett viktigt tillämpningsområde för forskningen är som utgångspunkt för den utbildning som måste bedrivas i kompetenshöjande syfte. Detta gäller både för grundläggande, längre utbildningar inför rekryteringar som för fortbildnings- och chefskurser. Särskilda satsningar behöver göras för att förbereda både militär och civil personal inför det växande antalet utlandstjänstgöringar. Detta fordrar även forskning och pedagogiskt utvecklingsarbete kring internationellt orienterade ämnen.

En förutsättning för en god innehållslig kvalitet i utbildningen av olika personalkategorier är att det finns en tillräcklig kår av högskolelärare som även är aktiva forskare inom området. Forskning om krishantering liksom försvarsrelaterad forskning behövs vid många av landets universitet och högskolor för att uppnå en sådan utbildningsbas. Samtidigt bör skapas förutsättningar för att forskningsbasen vid totalförsvarets egen högskola även inkluderar områden som berör det civila försvarets behov av kompetent personal inom myndigheter, kommuner och landsting, samt i företag likväl som inom frivilligorganisationer och andra relevanta folkrörelser.

10.3 Mellan kvalitet och relevans

All samhällsinriktad forskning står inför en balansproblematik. Å ena sidan behövs forskningens resultat inför ställningstaganden i komplexa och svårgripbara samhällsfrågor. En avtappning av kompetens efterfrågas av de som har till ansvar att genomföra reformer, prioritera mellan sakområden eller fastställa lösningar på olika samhällsproblem. Vid tillämpad forskning sammanfaller rollen som beställare med denna behovsstyrda efterfrågan på resultat som kan användas mer eller mindre operativt. Inte minst inom försvarssektorn med ett finansieringssystem av projektuppdrag, dialog mellan

beställare och utförare samt regelbundna avrapporteringar av milstolpar, betonas vikten av regelbunden och konkret kompetensavtappning.

Samtidigt kan ingen avtappning ske utan att även en gedigen och ofta långsiktigt verkande kunskapsuppbyggnad möjliggörs. Uthållighet är ett honnörssord i detta kompetenshöjande sammanhang. I detta kostnadskrävande värv kan mer kortsiktiga redovisningskrav innebära ett störande inslag, vilka undergräver eller fördröjer den för alla parter önskvärda kompetensuppbyggnaden inom ett forskningsområde. Betydelsen för samhället eller för området på sikt av en viss ny kunskap ställs mot ett mer omedelbart behov av att nyttiggöra forskningsresultat eller att använda tillgänglig kompetens inom ett fält. För den enskilde forskaren kan dessa motstridiga förväntningar vara svåra att hantera.

Det finns därför ett behov av större satsningar på tidiga insatser inom arbetet med att bygga upp kunskap även för det civila försvarets och den civila krishanteringens behov. Ett visst risktagande krävs för att öka sannolikheten av att dagens forskning kan ge ett nödvändigt kunskapsstöd i en osäker och komplex framtid. Det förutsätter möjligheter att säkerställa en öppenhet för kontrasterande analysperspektiv och olika problemställningar inom det civila försvaret och den civila krishanteringens områden.

Inom försvarsområdet används ofta begreppen forskning avseende kunskapsuppbyggande arbete och studier avseende avtappande verksamheter av olika slag. Studier kan delges i skrifter, föredragningar, informella dialoger eller vid akuta beslutsstödsbehov genom telefonremisser. Då formerna oftast är muntliga och informella är det svårt att säkra kvaliteten i budskapet. Forskningsresultat sprids främst i skriftlig form för att möjliggöra den kritiska, kvalitetssäkrande granskningen. Kunskaper delges dock även genom utbildningsinsatser, såsom föreläsningar, seminarier och läromedel. Expertuppdrag i utredningar eller beredningar bygger ofta på forskarbaserad kompetens inom ett område. På många sätt är det enklare att fastställa den vetenskapliga halten på en forskningsrapport, än att bedöma kvaliteten på ett mer löpande studiearbete.

Att både forskning och studier i princip behövs är inte omtvistat. Däremot föreligger en oenighet också inom försvarssektorn om prioriteringar mellan dessa tyngdpunkter, om forskares och analytikens tidsanvändning och om resursfördelningen och den organisatoriska profileringen mellan idealtyperna. Dessa diskussioner förefaller typiska för ett sektorsforskningsområde

med potentiella kunskapsbidrag inom policyrelevanta samhällsfrågor. De påminner till en del om debatten inom högskolan om resursfördelningen mellan grundutbildningsinsatser (avtappning) och forskningsprofileringar (uppbyggnad).

Vid sektorsforskning framstår det som särskilt väsentligt att det finns en god beställar- och mottagarkompetens. Inom problemfokuserad och delvis tillämpad forskning, till skillnad från disciplinutvecklande grundforskning, är i vissa avseenden de sedvanliga kvalitetsstärkande utslagningsmekanismerna satta ur spel. Inom forskning som finansieras av forskningsråd och av fakultetsmedel föreligger rätt tydliga spelregler, vilka syftar till att låta mindre goda insatser trängas ut av vetenskapligt mer framgångsrika forskare och projekt. Mekanismerna fungerar både vad gäller projektfinansiering och vid tjänstetillsättningar. Den forskarstyrda forskningen är naturligtvis inte utan problem, men i stort sett kan hävdas att detta sedan länge etablerade beställarsystem har över tid förmått lyfta fram det innovativa, nydanande och kvalitativt högtstående inom olika discipliner. Systemet har prövats över mycket lång tid och inom en rad vetenskapsområden. Av olika skäl har det inte prövats inom det svenska försvarsforskningsområdet.

Risken framstår som större att man inom ett sektorsforskningsfält får en skyddad enklav av projekt eller tillsvidareanställda forskare, som bland annat på grund av hög ämnesrelevans ges kontinuerlig finansiering utan att behöva utsättas för en kritisk vetenskaplig granskning. Både ämnesrelevans och vetenskaplig kvalitet måste säkerställas om ambitionen skall förbli solida kunskaper till sektorns nytta snarare än ett nyttiggörande av otillräckligt underbyggda studier. Avtappningen får inte prioriteras till prisets av att kunskapskällan sinar, utan att utföraren eller finansiären märker denna kvalitetsdränerande trend.

Sålunda bör man inom totalförsvarsforskningsområdet ställa än högre krav på en institutionaliserad beställar- och mottagarkompetens än vad som behövs inom den friare, och därmed mer utsatta, universitetsforskningen. I försvarssektorns nu rådande finansieringssystem med relativt korta uppdrag, ankommer det på beställare och mottagare inom regeringskansli och myndigheter att kunna hantera en rad svåra balansproblem, som man inom forskningsrådets och fakulteternas egenstyrda finansieringsform i stort har kunnat undvika.

10.4 Nuvarande hantering av forskning för det civila försvaret

Överstyrelsen för civil beredskap, ÖCB, har sedan ett antal år haft ansvar för att finansiera funktionsövergripande forskning samt för att samordna forskningen inom det civila försvaret. För att klara denna krävande uppgift har man stegvis byggt upp ett forskningsadministrativt system placerat inom myndighetens analysenhet. Anslag har utlysts i regelbundna cykler och forskare vid universitet och sektorsforskningsinstitut har på olika sätt uppmuntras att inkomma med ansökningar. Ett stort antal ansökningar har varje år behandlats och många har avförts genom denna relativt krävande beredningsprocess. Förutom denna öppna ansökningsform har ett antal ramforskningsprogram etablerats inom för verksamheten prioriterade områden. Dessa fleråriga satsningar på ämnen och miljöer har utarbetats i dialog mellan utförare och beställare. Både vid universitet och vid institut, som t.ex. FOI (FOA), har dylika program etablerats. Under senare år har man i högre grad även ägnat implementeringsfrågorna en hel del möda. Det är välkänt inom forskningsrådssfären att det är svårare att bygga upp en mottagar- och uppföljningskompetens än att skapa en god beställarkompetens. Forskningsimplementering är nu ett prioriterat arbetsområde inom den ansvariga enheten.

ÖCB har arbetat längs två huvudspår i sin ambition till en god beredning av ansökningar. För att säkerställa ämnesrelevansen har många av myndighetens företrädare, från de relevanta sakenheterna, engagerats i beredningsarbetet av ansökningar och i uppföljning av forskningsresultat. Därtill har en särskild referensgrupp etablerats för att bland de många inkommande ansökningarna lyfta fram det som kan anses ha relevans för verksamheten. I detta arbete har även företrädare för de funktionsansvariga myndigheterna engagerats. Antingen har de ingått i referensgruppen eller har de fått ansökan på remiss för yttrande. Vid forskardagar, temakonferenser och andra utåtriktade aktiviteter har forskningsresultat presenterats för olika avnämningarkategorier och kontakter har skapats mellan dessa och forskarna inom respektive problemområde. Småskrifter har distribuerats och artiklar har publicerats i Beredskap och andra magasin. De av ÖCB finansierade forskarna har engagerats på många sätt i dessa försök att nå ut med de för verksamheten nyttiga rönen.

Beredningsarbetet har även inkluderat ambitionen att säkra den vetenskapliga kvaliteten bland de finansierade projekten. Ett veten-

skapligt råd inrättades tidigt med seniora ledamöter från olika relevanta forskningsmiljöer och från hela landet. Rådet tar ställning till projektens forskningsbarhet och potentiella bidrag utifrån vedertagna vetenskapliga kriterier. Här ställs analys- och metodfrågor i centrum, liksom utförarens kvalifikationer för uppgiften. Arbetet inom detta råd liknar mycket det beredningsarbete som utförs vid de disciplinorienterade forskningsråden. Ofta har dessa erfarna och framåtblickande forskare även möjlighet att lyfta fram värdefulla kunskapsbidrag av potentiell områdesrelevans. Det vetenskapliga rådets ledamöter har inte sällan en god överblick över framtida kunskapsbehov.

Den planeringsmyndighet som utredningen föreslår bör få till uppgift att ta ett samlat grepp om dessa frågor och verka för en förstärkning av forsknings- och utvecklingsinsatserna inom civilförsvarets och den civila krishanteringens område. Myndigheten bör som framhållits tilldelas medel för att också kunna uppträda som beställare av forsknings- och utvecklingsinsatser. Förmågan att kunna utnyttja kompetenser från olika akademiska områden tillsammans med annan relevant kunskap kommer att bli en viktig framgångsfaktor i framtiden.

10.5 Förslag till överblick och kvalitet

Hur kan ett forskningsfinansieringssystem organiseras för det civila försvarsområdet och den civila krishanteringens område så att man kan uppnå flera önskvärda betingelser?

Skapa pluralism och vidsynthet men även möjliggöra syntes och överblick.

Uppmuntra framåtblickande, nyfikenhetsbaserade upptäckter i kunskapsuppbyggande syfte samt säkra en mer regelbunden avtappning inför mer omedelbara policybehov.

Säkra både vetenskaplig kvalitet och problemrelevans.

Skapa en vetenskaplig grund både för ett analytiskt beslutsstöd och som bas till utbildningar för att främja personalförsörjningen.

Undvik ämnesbredd till priset av bristande djup.

Dra fördel av det internationella kunskapsutbudet utan att tappa kontakt med inhemska frågeställningar och utbildningsbehov.

Möjliggör en förnyelse av perspektiv och profilinriktningar utan att förlora de betydande kunskaper och erfarenheter som etablerade institut och forskargrupper besitter.

Följande behöver åstadkommas i närtid:

1. En mångfald av forskargrupper måste uppmuntras. Existerande, de facto monopolställningar i anslag eller beställarrelationer bör brytas och öppnas för konkurrens mellan många möjliga utförare. Både universitet och högskolor samt sektorns specialforskningsinstitut engageras på lika villkor.
2. Många engageras som beställare och mottagare av forskning och studier. Vissa finansiärer eller anslagspotter kan betona långsiktig kunskapsuppbyggnad, medan andra kan prioritera kortare studieuppdrag. En del vill lyfta fram vissa problemområden, medan andra ser kunskapsbehoven på andra prioriterade fält. Dessa finansiärer får konkurrera om de bästa forskarna och projektplanerna. En mångfald av intressenter – finansiärer och utförare – inom sektorn behöver skapas.
3. Varje finansiär avkrävs ett ansvar för att bygga upp en god kompetens inför uppgiften. Beställarkompetensen skall omfatta både förmåga till relevansbedömning samt till vetenskaplig prövning. Mottagarkompetensen måste gå utöver kameral överblick och inte minst innebära en förmåga till sakmässig uppföljning av forskningsresultaten. Regeringskansliet förväntas antingen föregå med gott exempel som en bland flera kompetenta forskningsfinansiärer, eller delegera det operativa ansvaret för denna krävande verksamhet.
4. Denna mångfald av utförare och beställare knyts samman i ämnes- eller problemfokuserade nätverk tvärs över myndigheter och forskargrupper. Nätverk kan skapas med inriktning mot discipliner, som samhällsvetenskap, beteendevetenskap, teknik och samhälle, eller alternativt mot problemområden som infrastrukturfrågor, krishantering, och internationellt fredsfrämjande. Nätverken skall inte begränsas till informationsutbyte på hög nivå, utan vara arbetande grupper med aktiva forskare och forskningsansvariga som kan bidra till att skapa förmåga. Nödvändig överblick och uppföljning av initiativ skapas genom dialog och uppdrag till arbetsgrupper inom dessa nätverk.
5. En sekretariatsfunktion krävs för att driva arbetet inom nätverken framåt, initiera studiegrupper, föreslå nya problemområ-

den, ordna seminarier och konferenser. Utan ett pådrivande sekretariat lär inte nätverken fungera som arbetande grupper med syfte att lyfta fram överblick och perspektiv på tvärs över olika forskargrupper och mellan dessa och många potentiella beställare och användare. Det civila försvarets och den civila krishanteringens verksamheter spänner över en ansenlig ämnesbredd och engagerar många forskningsmiljöer. Därför är denna institutionalisering av nätverkens gemensamma nod ett nödvändigt inslag.

6. Sekretariatet skall fullgöra en rad uppgifter som påminner om ett forskningsråds ansvar, men i en mer blygsam omfattning. Man skall notera att de traditionella forskningsråden aldrig var de enda finansierarna inom ett vetenskapsområde, utan de har haft uppgiften att skapa överblick och förnyelse. Sekretariatet bör:

Säkra en strategisk överblick inom det civila försvarets och den civila krishanteringens ämnesmässigt breda och komplexa verksamhetsområde.

Säkra en resursmässig samordning över områdets många beställare och utförare.

Säkra en koppling till näringslivet och det civila samhällets nätverksaktörer.

Säkra varje nätverks koppling till den internationella forskningsfronten.

Säkra förnyelsen av kompetens och generationsskiften inom forskarkåren genom koppling till utbildande institutioner.

Säkra relevansbehov och användarperspektiv på hög nivå genom koppling till demokratiskt sammansatta beredningar och nationella styrorgan.

Förslaget ovan tar sin utgångspunkt i behovet av att skapa incitamentsstrukturer som främjar områdesrelevant forskning av god kvalitet.

Den myndighetsdominerade styrningen bör kombineras med en mer forskarstyrd arbetsform, där nya impulser och problemställningar kontinuerligt flyter upp inom beredningsarbetet. Detta förefaller som särskilt viktigt inom det en sådan mångfacetterad och decentraliserad verksamhet som det civila försvaret och civil krishantering utgör. Därtill bör man inom denna sfär engagera forskargrupper vid landets universitet och högskolor. Sådana för

kunskapsuppbyggnaden viktiga och pluralistiska konstellationer låter sig inte enkelt underordnas ett myndighetsbaserat styrsystem.

Lika viktigt som att uppnå central överblick och en övergripande strategisk inriktning av försvarsforskningen är att stimulera nydanande och ofta utmanande forskarinsatser. Dessa kunskapskorn kan få stor betydelse i framtiden, även om de inom stundens ofta snäva relevanskriterier framstår som udda. Risken med att enbart lita till myndighetsbaserade strategidokument är att man uppnår effektivt verkande forskning, men på sikt tappar den nödvändiga kunskapsförnyelsen.

11 Tillsyn i säkerhetsarbetet

11.1 Inledning

Det finns ett flertal samhällsviktiga verksamheter, bl.a. inom teknisk infrastruktur och transportsektorn, som är gränssättande för säkerheten och beredskapen och för förmågan att hantera allvarliga krissituationer. En viktig del i säkerhetsarbetet är därför dels föreskrifter som reglerar riskbetonade verksamheter, dels föreskrifter som anger grundläggande säkerhetskrav. Därutöver finns ett behov av att kontrollera att föreskrifterna efterlevs och att föreskrifternas resultatförmåga utvärderas. I detta säkerhetsarbete har tillsynsfunktioner en viktig roll. I det följande redogör utredningen för ett antal viktiga förutsättningar för att åstadkomma en effektiv tillsyn. Vid en genomgång av tillsynsfunktioner inom olika områden kan man konstatera att det finns olika organisatoriska lösningar, men det finns även andra skillnader mellan tillsynsorganens förutsättningar för att utöva tillsyn. Utredningen har bl.a. värderat frågan om betydelsen av att en tillsynsfunktion är juridiskt, ekonomiskt och administrativt fristående i förhållande till den vars verksamhet man utövar tillsyn över.

11.2 Begreppet tillsyn

Det har i tidigare utredningar konstaterats att det inte finns en enhetlig definition av begreppet tillsyn i lagar och andra föreskrifter. Det finns också skilda uppfattningar om vilka uppgifter som bör ingå i den mest ändamålsenliga tillsynsverksamheten.¹ I en rapport till expertgruppen för studier i offentlig ekonomi framhålls att det är orealistiskt att ta fram en enda allmängiltig definition av be-

¹ Statlig tillsyn – ett förvaltningspolitiskt styrmedel RRV 1996:10, s 10. I prop. 1997/98:45 till miljöbalken innefattas med begreppet tillsyn såväl inspektion, åtgärder för att åstadkomma rättelse som förebyggande åtgärder i tillsynsarbetet

greppet tillsyn, men att det kan vara meningsfullt att skilja mellan två huvudsakliga användningar av ordet – det vida och det snäva tillsynsbegreppet.² Det vida tillsynsbegreppet innefattar de olika åtgärder som vidtas för att intentionerna i lagstiftningen skall genomföras. Tillsyn blir här ungefär liktydigt med implementering av lagstiftningen och innefattar allt från utfärdande av föreskrifter som preciserar lagarna till inspektions- och informationsverksamhet samt förprovning och utfärdande av tillstånd. Det snäva tillsynsbegreppet innefattar endast handlingar som består i att dels undersöka om enskilda företag m.fl. efterföljer lagar och regler, dels vidtar åtgärder för rättelse av uppdagade brister i efterlevnaden. Tillsyn blir här ungefär liktydigt med inspektionsverksamhet.

Regeringen har den 21 september 2000 (dir. 2000:62) beslutat att tillkalla en utredare med uppdrag att utreda hur den statliga tillsynen kan göras till ett tydligare och effektivare förvaltningspolitiskt instrument som bättre bidrar till kontrollen och genomförandet av demokratiskt fattade beslut (Ju 2000:06). I ett första steg har utredaren för avsikt att kartlägga all lagstiftning innehållande begreppet tillsyn, vilka myndigheter som har tillsynsansvar m.m.

I följande beskrivning tar utredningen i första hand fasta på hur man har utformat den tillsyn – i vid mening – som centrala myndigheter, länsstyrelser och kommuner utövar och som riktas mot det omgivande samhället. Det är inte en uttömmande redovisning av hur tillsynen har organiserats i samhället, utan organisation och uppgifter för tillsynsmyndigheter kommer att presenteras kortfattat liksom den lagstiftning som tillsynen grundar sig på. Flertalet av dessa tillsynsmyndigheter har dels till uppgift att utfärda föreskrifter, att ställa villkor i samband med koncession för viss verksamhet, dels att kontrollera att lagar och andra föreskrifter efterlevs samt ge information och rådgivning. För en del av myndigheterna är arbetet helt inriktat på säkerhetsfrågor, t.ex. inspektionerna på trafikområdet, men för andra utgör fastställande och granskning av säkerhetskrav endast en del av uppgifterna och en stor del av resurserna används för att kontrollera att det råder en fri konkurrens, att prissättning är rimlig m.m. Den övergripande uppgiften för dessa myndigheter är att främja utvecklingen inom ett särskilt verksamhetsområde. Exempel på sådana tillsyns-

² Ds 1998:50, s 57 f. Att se till eller titta på – om tillsynen inom miljöområdet (Rapport till ESO, Expertgruppen för studier i offentlig ekonomi)

myndigheter är Post- och telestyrelsen och Statens energimyndighet.

Utredningen beskriver här den tillsyn som kan sägas utgöra en del av ett statligt åtagande. Det är viktigt att påpeka att varje verksamhetsutövare i första hand har ett eget ansvar för sin verksamhet och att detta ansvar i sig omfattar olika former av kontroller samt intern revision. Den tillsyn som här beskrivs skall således utgöra en oberoende kontroll av verksamheten. Utöver denna tillsyn tillkommer de enskilda medborgarnas egen kontroll och den granskning som utförs av media.

11.3 Viktiga förutsättningar för att skapa en effektiv tillsyn

Riksdagens revisorer har i olika utredningar framhållit att viktiga förutsättningar för statlig tillsyn är lagstiftningens utformning, förekomsten av relevanta tillämpningsföreskrifter samt tillsynsorganets ställning, resurser, kunskaper om det som skall tillses och uppläggningsen av arbetet.³ Revisorerna har även understrukit vikten av att man i samband med samhällsorganisatoriska förändringar anpassar tillsynens omfattning och inriktning till de nya förutsättningarna. Här nedan ges en kort sammanfattning av dessa synpunkter.

En klar och tydlig lagstiftning är grundläggande framför allt beträffande ansvarsfördelning och vad tillsynsansvaret omfattar och innebär. I lagstiftningen anges vad som skall tillses, vem som har ansvaret för tillsynen och vilka befogenheter en tillsynsmyndighet har. Ofta anges också verksamhetsutövarens ansvar och vilka sanktionsåtgärder som kan bli aktuella i de fall brister konstateras. Inom flera områden har en central tillsynsmyndighet även till uppgift att meddela föreskrifter.

När det gäller en genomförd granskning av tillsynsorganen på transportområdet har revisorerna konstaterat att det kan vara svårt för inspektionerna att upprätthålla självständighet i sin myndighetsutövning, eftersom de till stor del ansågs vara beroende av andra myndigheter för sin normgivning, planering och ekonomi.⁴ För beslutsfattare och allmänheten framstod inspektionernas ställning som oklar och deras självständighet kunde därmed sättas i fråga, både av allmänheten och av företrädare för verksamhetsut-

³ Se bl.a. *Tillsyn - innebörd och tillämpning*, förslag 1994/95:RR9

⁴ 1994/95:RR9, s 7

övarna. Revisorerna har vidare i upprepade granskningar kommit fram till att tillsynens oberoende och integritet behöver förstärkas, att det är viktigt att tillsynsansvaret ligger utanför verksamhetsutövarens kontroll och påverkan. Revisorerna bedömer att ett sätt att åstadkomma en mera självständig tillsyn är att skapa en tillsynsfunktion som är organisatoriskt fristående från den verksamhet som skall tillses samtidigt som de konstaterar att det kan innebära svårigheter att upprätthålla kunskap och kompetens hos ett tillsynsorgan när man inte har samma närhet till verksamhetsutövaren.

Det kan finnas motstridiga intressen inom den myndighet som skall utöva tillsyn. Utredningen konstaterar här att det t.ex. kan finnas en motsättning mellan tillsynsuppgifter som hänförs till intresset av att tjänster skall tillhandahållas till låga kostnader och tillsynsuppgifter som består i att ställa krav på säkerhet. Energimyndigheten är ett exempel på en tillsynsmyndighet där en sådan motsättning kan uppkomma, men det finns på ett flertal områden dubbla roller för tillsynsmyndigheter på så sätt att myndigheten såväl skall främja utvecklingen inom ett visst område samtidigt som den har till uppgift att övervaka att företag m.fl. tar tillräcklig hänsyn till säkerhetsaspekter. I de fall säkerhetsmålen är svårbestämbara är problemet än mer allvarligt. En viktig förutsättning för en effektiv tillsyn är således att tillsynsorgan och verksamhetsutövare har klart för sig vilka förväntningar statsmakterna har på deras arbete.

Till sist konstateras att ett sanktionssystem kan bidra till en effektivare tillsyn och bättre lagefterlevnad.

11.4 Exempel på hur tillsynsuppgifter har reglerats på olika områden

Kärnenergiområdet

Ett område där en olyckshändelse kan få ytterst allvarliga konsekvenser är kärnenergiområdet. Att säkerhetsarbetet här är av största vikt återspeglas bl.a. i de författningar som reglerar tillsynen av kärnenergiaktivitet. För kärnteknisk verksamhet krävs tillstånd som meddelas av regeringen eller Statens kärnkraftinspektion (SKI). Den som har fått tillstånd att bedriva kärnteknisk verksamhet har det fulla säkerhetsansvaret för driften vid anläggningen, men SKI har till uppgift att se till att ägaren tar sitt

ansvar och bedriver verksamheten på ett säkert sätt. Vid tillståndsprovning kan SKI meddela de villkor som krävs med hänsyn till säkerheten. Det är SKI som utövar tillsynen av efterlevnaden av kärntekniklagen (1984:3) och av de villkor eller föreskrifter som meddelats med stöd av lagen. SKI samarbetar i vissa frågor med Statens strålskyddsinstitut (SSI) som bl.a. har till uppgift att övervaka att strålskyddsbestämmelserna efterlevs. Det finns möjlighet att besluta om förelägganden och förbud förenat med vite samt att vidta åtgärder på tillståndshavarens bekostnad och att återkalla tillstånd. Därutöver finns i kärntekniklagen särskilda straffbestämmelser. Enligt utredningen är det tydligt att SKI i sin tillsynsroll har en mycket stark ställning gentemot verksamhetsutövarna vilket innebär att myndigheten kan agera kraftfullt i säkerhetsfrågor.

Teleområdet

På teleområdet har Post- och telestyrelsen (PTS) som regleringsmyndighet – fristående från de verksamma teleoperatörerna – ansvar för tillsynen över telemarknaden. Bestämmelser om tillsyn på teleområdet finns i telelagen (1993:597) och teleförordningen (1997:399). PTS skall pröva frågor om tillstånd samt utöva tillsyn över efterlevnaden av telelagens bestämmelser och de föreskrifter och villkor som meddelats med stöd av lagen.⁵ PTS tillsynsuppgifter är inte endast inriktade på att säkerställa en tillräcklig ambition för säkerhetsåtgärder. Bestämmelserna i telelagen syftar även till att enskilda och myndigheter skall få tillgång till effektiva telekommunikationer till lägsta möjliga samhällsekonomiska kostnad. För att kunna utöva tillsyn har PTS rätt att på begäran erhålla det material som behövs och kan meddela de föreskrifter och förbud som behövs för efterlevnaden av lagen. Utöver bestämmelserna i telelagen, teleförordningen berörs teleoperatörerna av olika tillståndsvillkor. Dessa villkor har utfärdats med stöd av telelagen och innebär en utveckling, och i vissa fall ett förtydligande, av på vilket sätt olika skyldigheter skall fullgöras. PTS är därutöver beredskapsmyndighet för telekommunikationer och kan meddela föreskrifter om den framtida planeringen för totalförsvarets behov av telekommunikationer.⁶ PTS har enligt telelagen även möjlighet att meddela föreskrifter om

⁵ 57 § telelagen och 2 § teleförordningen

⁶ 65 § telelagen och 17 § teleförordningen

avgifter för beredskapsåtgärder på telekommunikationsområdet. Enligt utredningens uppfattning har PTS ett tydligt tillsynsansvar gentemot verksamhetsutövarna inom telekommunikation. Telelagen stadgar att den som inom ett allmänt tillgängligt telenät tillhandahåller teletjänster eller nätkapacitet skall se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet. PTS får meddela närmare föreskrifter om sådana krav.

Miljöbalken

Tillsynen över efterlevnaden av föreskrifter enligt miljöbalken är uppdelad i operativ tillsyn – sådan tillsyn som utövas direkt gentemot den som bedriver en verksamhet eller vidtar en åtgärd – och tillsynsvägledning – sådan tillsyn som består i utvärdering, uppföljning och samordning av den operativa tillsynen samt stöd och råd till de operativa tillsynsmyndigheterna.⁷ Den operativa tillsynen utövas av en särskild kommunal nämnd eller länsstyrelsen medan ansvaret för tillsynsvägledning tillkommer en rad olika centrala myndigheter beroende på verksamhetsområde.

Dammsäkerhet

Inom dammsäkerhetsområdet skall den som är underhållsskyldig för en dammbyggnad själv utarbeta och följa rutiner för egenkontroll.⁸ Den underhållsskyldige skall vidare känna till de konsekvenser som kan bli följden av felfunktioner och använda bästa möjliga teknik för att undvika skador. Om ett dammbrott likväl skulle inträffa, är den underhållsansvarige ansvarig för de skador som orsakas. Uppförande av en damm liksom ändring och lagning av en damm är tillståndspliktig vattenverksamhet. En ansökan om tillstånd prövas av miljödomstol. Länsstyrelserna har det operativa tillsynsansvaret⁹ för dammsäkerheten. Sedan år 1998 har Affärsverket svenska kraftnät en samordnande roll inom områdena dammsäkerhet och höga flöden. Enligt sin instruktion skall Svenska kraftnät främja dammsäkerheten i landet och i enlighet

⁷ 3 § förordning (1998:900) om tillsyn enligt miljöbalken

⁸ Rutiner för dammägarnas egenkontroll beskrivs i de övergripande riktlinjer för dammsäkerhet som Svenska Kraftverksföreningen har antagit (RIDAS). Även gruvindustrin har beslutat att i tillämpliga delar följa dessa riktlinjer

⁹ För det fall tillsynsansvaret inte överlätts till kommunerna, jfr Förordning (1998:900) om tillsyn enligt miljöbalken

därmed utarbetar Svenska kraftnät en handbok om egenkontroll och tillsyn med länsstyrelserna som primär målgrupp. I instruktionen anges vidare att Svenska kraftnät skall följa utvecklingen vad avser dammsäkerhet i landet, verka för att höga flöden som kan orsaka skador begränsas vid driften av dammar och regelbundet rapportera till regeringen om utvecklingen. Till stöd för arbetet med dammsäkerhetsfrågor har Svenska kraftnät ett rådgivande organ, Dammsäkerhetsrådet.¹⁰ Svenska kraftnät är dock inte nämnt i tillsynsförordningen som tillsynsvägledande utan i stället anges Naturvårdsverket som tillsynsvägledande myndighet. Länsstyrelserna har på uppdrag av Statens räddningsverk bildat älvvisa samordningsgrupper för de större vattendragen i landet. Dessa älvgrupper är viktiga för att skapa en regional nätverks- och kunskapsuppbyggnad vad gäller höga flöden och dammsäkerhet. I grupperna ingår nyckelpersoner från länsstyrelser, kommuner, dammägare, Vägverket, Banverket m.fl. Älvgrupperna är inte i sig operativa, men de deltagande organisationerna och myndigheterna är operativa var för sig inom sitt område. Länsstyrelserna har en naturlig roll som operativt tillsynsansvarig för dammsäkerhet¹¹ men trots ambitioner finns det problem på grund av att resurserna på länsstyrelserna inte är tillräckliga för att utöva den tillsyn som erfordras. En lösning kan vara att de tjänster som erfordras delas av flera länsstyrelser. Därutöver anser utredningen att det kan finnas skäl för en tydligare tillsynsvägledning för dammsäkerhet på central nivå än den främjanderoll som Svenska kraftnät har idag.

Allvarliga kemikalieolyckor

Lagen (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor tillkom i samband med att det nya Seveso-direktivet¹² skulle införlivas i svensk rätt. Lagen föreskriver att för visst slag av verksamheter – där farliga ämnen förekommer i mängder som motsvarar eller överstiger särskilt angivna mängder – skall verksamhetsutövaren vidta särskilda åtgärder för att förebygga risker för allvarliga kemikalieolyckor och

¹⁰ Dammsäkerhetsrådet ersatte den tidigare Dammsäkerhetsnämnden som haft i uppgift att lämna principiella, skriftliga rekommendationer för underhåll och tillsyn av dammar

¹¹ Länsstyrelserna är tillsynsansvarig för den kommunala räddningstjänsten och har i vissa situationer dessutom en operativ ledningsroll inom räddningstjänsten. Länsstyrelserna svarar även för den regionala samordningen av den fysiska planeringen och granskar översiktsplaner ur säkerhetssynpunkt

¹² Rådets direktiv (96/82/EEG) om åtgärder för att förebygga och begränsa följderna av allvarliga olyckshändelser där farliga ämnen ingår (Seveso II)

begränsa följderna för människors hälsa och miljö i de fall en allvarlig kemikalieolycka har inträffat. Verksamhetsutövarens skyldigheter omfattar bl.a. att anmäla verksamheten och att utarbeta ett handlingsprogram för hur allvarliga kemikalieolyckor skall förebyggas. Regeringen kan därutöver föreskriva att det skall vara förbjudet att utan tillstånd anlägga en verksamhet som omfattas av lagen, även om tillstånd inte krävs enligt miljöbalken. En ansökan om tillstånd skall prövas av miljödomstol, men regeringen får föreskriva att ansökan om tillstånd för vissa slag av verksamheter skall prövas av länsstyrelsen. För vissa verksamheter får regeringen föreskriva att verksamhetsutövaren skall upprätta säkerhetsrapport och intern plan för räddningsinsatser. Det är Räddningsverket, länsstyrelserna och kommunerna som utövar tillsyn över att lagen och de föreskrifter som har meddelats med stöd av lagen följs. Länsstyrelserna och kommunerna skall ha tillsyn över verksamhet som omfattas av tillståndsplikt enligt miljöbalken i enlighet med den ansvarsfördelning för tillsynen av miljöfarlig verksamhet som följer av miljöbalken. Därutöver har Räddningsverket ett samordnande, kontrollerande och uppföljande ansvar. Tillsynsmyndigheterna har rätt att få tillträde till en verksamhet samt rätt att få de upplysningar och tillgång till de handlingar som behövs för tillsynen. De har befogenhet att meddela förelägganden och förbud, vilka får förenas med vite. Tillsynsmyndigheten kan även – vid underlåtelse att efterfölja ett föreläggande – vidta åtgärden på verksamhetsutövarens bekostnad.

Transportområdet

Inom transportområdet är tillsynen på olika sätt knuten till infrastrukturhållaren. Sjöfartsinspektionen, Luftfartsinspektionen och Järnvägsinspektionen har alla tillsynsuppgifter och de är inrymda i Sjöfartsverket, Luftfartsverket respektive Banverket. Inspektionerna har även ett visst tillsynsansvar över dessa myndigheters verksamheter.

Riksdagens revisorer har konstaterat att utvecklingstendenserna och problemen till stor del är gemensamma för de olika transportslagen. Det gäller inslagen av avreglering, egenkontroll, nya former för teknisk provning och kontroll, internationalisering samt behovet av tydliga gränser mellan affärsmässig produktion och myndighetsuppgifter såsom tillsyn.

Frågan om behovet av tydliga gränser mellan producerande verksamhet och myndighetsuppgifter sammanhänger med hur man skall säkerställa att sektors- och myndighetsuppgifter kan utövas självständigt gentemot verksamhetsutövare (samt för att uppnå en effektiv förvaltning och produktion). Under slutet av 1990-talet har frågan om rollkonflikter inom trafikverken föranlett flera utredningar inom Regeringskansliet. Regeringen har analyserat trafikverkens verksamhetsstrukturer och sökt eliminera eventuella konflikter mellan producerande verksamheter och sektorsuppgifter som säkerhetsfrågor och tillsyn.¹³ I dessa utredningar har man i huvudsak identifierat tre olika roller som gäller säkerhet, produktion respektive sektorsverksamhet. I den rapport som avsåg Luftfartsverket menade den anlitade konsulten att det inte var något problem för Luftfartsverket att hantera de olika rollerna, eftersom de inom verket var ansvarsmässigt separerade från varandra under generaldirektörsnivån. Däremot ansågs det vara ett problem för Luftfartsverket att det inom luftfartsmarknaden fanns misstankar om att verket i sin sektorsroll skulle kunna gynna verket i dess producentroll. I den rapport som avsåg Sjöfartsverkets verksamhetsstruktur¹⁴ fann konsulten att konflikterna mellan verkets olika roller hade begränsad omfattning. Sjöfartsverket hade enligt rapporten få kommersiella intressen att bevaka, och verket befann sig inte i någon konkurrenssituation gentemot andra intressenter som t.ex. kommuner. Rollkonflikterna ansågs dock utgöra ett problem bl.a. genom att det skapas en osäkerhet om självständigheten i verkets myndighetsbeslut, dvs. att hänsyn tas till det egna produktionsintresset. För att minska följderna av rollkonflikter lämnades följande alternativ: (1) tydligare mål och bättre rutiner för att hantera målkonflikter, (2) en organisation baserad på producent-, sektors- respektive regulatorrollen, och (3) Sjöfartsinspektionen som en separat myndighet.¹⁵ Även Järnvägsinspektionens roll har utretts och vid det tillfället menade regeringen att den gällande organisationen på ett ändamålsenligt och tillfredsställande sätt gav det oberoende i säkerhetsfrågor som inspektionen måste ha. Att ombilda inspektionen till en egen

¹³ Se bl.a. *Översyn av Luftfartsverkets verksamhetsstruktur*, Näringsdepartementet, 1999-11-18

¹⁴ Översyn av Sjöfartsverkets mål och roller, 1999-10-08

¹⁵ Vid remissbehandlingen framkom dels synpunkter om att Sjöfartsinspektionen borde bli en självständig myndighet, eftersom rollerna då skulle kunna renodlas och inspektionen skulle då enbart hantera säkerhetsrelaterade roller, dels synpunkter om att målkonflikter är vanliga i offentlig verksamhet och att genuina målkonflikter inte försvinner i och med att ansvaret för olika mål delas upp på olika organ

myndighet skulle enligt regeringens bedömning medföra stora ekonomiska nackdelar och dessutom leda till en mer omfattande administration.

Tidigare har Inspektionskommittén föreslagit att Luftfartsinspektionen och Järnvägsinspektionen skulle ombildas till egna myndigheter för att tydligheten i de båda inspektionernas myndighetsutövning skulle kunna öka.¹⁶

Riksdagens revisorer har nyligen lämnat ett förslag angående Sjöfartsinspektionens tillsyn innefattande bl.a. att uppgifter rörande tillsyn och säkerhetsnormer bör läggas direkt på inspektionen i lagstiftningen för att förtydliga Sjöfartsinspektionens ställning.¹⁷ Vid Trafikuskottets behandling av förslaget konstaterade utskottet att man delade revisorernas uppfattning¹⁸ om att Sjöfartsinspektionens självständighet och integritet i förhållande till Sjöfartsverket och omvärlden måste säkerställas så långt detta är möjligt. Utskottet framhöll att det finns ett principiellt integritetsproblem inbyggt i nuvarande organisationsform, men medgav samtidigt att en samlad organisation innebär fördelar. Sammanfattningsvis följde utskottet revisorernas förslag om att inspektionens ställning – inom ramen för en oförändrad organisatorisk hemvist inom Sjöfartsverket – bör tydliggöras i den lagstiftning som reglerar Sjöfartsinspektionens verksamhet. I avvaktan på att så sker var utskottet inte berett att förorda att Sjöfartsinspektionen skiljs ut från Sjöfartsverket.

I samband med sin granskning konstaterar riksdagens revisorer att även om det kan vara en fördel för tillsynsorgan med närhet till verksamhetsutövarna, så har revisorerna i flera tidigare granskningar kommit fram till att tillsynens oberoende och integritet behöver stärkas. Jämfört med Järnvägsinspektionen och Luftfartsinspektionen är Sjöfartsinspektionen den inspektion som är minst självständig i förhållande till värdmyndigheten. Både Luftfarts-

¹⁶ *En översyn av luft-, sjö- och spårtrafikens tillsynsmyndigheter (SOU 1996:82)*

Inspektionskommittén lämnade inte samma förslag för sjöfartsområdet eftersom Sjöfartsverkets verksamhet till övervägande del är inriktad på sjösäkerhetsarbete. Enligt kommittén hade inte heller frågan om oberoende och självständighet samma aktualitet eller betydelse som för Luftfartsinspektionen och Järnvägsinspektionen, eftersom Sjöfartsverket inte var infrastrukturhållare på samma sätt som Luftfartsverket och Banverket.

¹⁷ Riksdagens revisorers förslag 2000/01:RR8. Granskningen avsåg Sjöfartsinspektionens tillsyn; i första hand tillsynens innehåll och uppläggning samt rapportering och analys av tillsyn och olyckor. Granskningen gällde även förutsättningarna för inspektionens tillsyn, och hur inspektionen använt sig av dem. Granskningen omfattade särskilt tillsynsverksamheten under perioden 1995 – 1999 i syfte att se hur inspektionen åtgärdat tidigare påtalade brister. På ett par områden konstaterades att tillsynen inte var så effektiv som kunde önskas.

¹⁸ Trafikuskottets betänkande 2000/01:TU8

inspektionen och Järnvägsinspektionen har en tydligare ställning i lagstiftningen.¹⁹

Elområdet

Utredningen har i tidigare avsnitt beskrivit det svenska elsystemet, varvid framhållits att säkerheten i elförsörjningen behöver förbättras. Organisationen IEA (International Energy Agency)²⁰ har under år 2000 gjort en landstudie av Sveriges energipolitik och i samband därmed lämnat ett antal rekommendationer. En av dessa är vikten av en oberoende tillsyn på energiområdet och inom elförsörjningen. I rapporten konstateras att Näringsdepartementet har ansvaret för att utveckla riktlinjer på energiområdet och att Energimyndigheten har ansvaret för att riktlinjerna förverkligas. IEA föreslår att regeringen bör överväga att ytterligare förstärka den funktion inom Energimyndigheten som svarar för reglering av energiområdet genom att funktionen flyttas till en organisation som är helt skild från departementet och Energimyndigheten.

I rapporten konstateras vidare att nätavdelningen inom Energimyndigheten självständigt – inom ramen för ellagen – utövar tillsyn av elnäten. IEA menar dock att regeringen har en dubbel roll eftersom man meddelar föreskrifter för elindustrin samtidigt som staten är ägare till ett av de största företagen. I rapporten förordas en oberoende regleringsmyndighet vilket skulle ge ett avstånd mellan normgivare/tillsynsfunktion och marknadsaktörerna. Vidare rekommenderas en översyn av nätavdelningens roll för att identifiera möjligheter för att stärka dess makt och oberoende vilket skulle förbättra tillsynens kvalitet.

Elsäkerhetsverket är tillsynsmyndighet såvitt gäller frågor om elsäkerhet. Elsäkerhetsverket har befogenhet att ingripa när elanläggningar befaras vara farliga att använda och dess uppgift är att se till att det inte uppkommer skador på människor, djur eller egendom.

Svenska kraftnät har systemansvaret för el, vilket innebär det övergripande ansvaret för att elektriska anläggningar samverkar

¹⁹ Övergången till civil bemanning på sjömättnings- och isbrytarfartyg innebär att Sjöfartsverket inrättar en rederifunktion samtidigt som Sjöfartsverket kommer att ha ansvar för tillsynen av fartygen. De ändrade ansvarsförhållandena innebär att verket i viss mån tillser sig självt, vilket självfallet innebär komplicerade avvägningar mellan ekonomiska och andra bedömningar samt frågor om säkerhet.

²⁰ IEA är ett självständigt organ som tillkom 1974 inom ramen för OECD (Organisation for Economic Co-operation and Development) för att implementera ett internationellt energiprogram.

driftsäkert så att balans inom hela eller delar av landet kortsiktigt upprätthålls mellan produktion och förbrukning av el. Svenska kraftnät är även elberedskapsmyndighet och fattar som sådan beslut om erforderliga beredskapsåtgärder.

Med undantag för Svenska kraftnäts och Elsäkerhetsverkets ansvarsområden utövas tillsynen över ellagen och av föreskrifter och villkor som meddelats med stöd av lagen av Energimyndigheten i egenskap av nätmyndighet.²¹ Nätmyndighetens tillsyn omfattar bl.a. skäligheten av koncessionshavarens tariffer.

Tillsynsmyndigheterna, dvs. Svenska kraftnät, Elsäkerhetsverket och Energimyndigheten, får meddela de förelägganden som behövs samt förena dem med vite. I fråga om elsäkerhet och driftsäkerhet har tillsynsmyndigheterna befogenhet att förordna om rättelse på vederbörandens bekostnad eller att förbjuda tillhandahållande eller användning av elmaterial m.m. Energimyndigheten kan dock som sista åtgärd endast återkalla en koncession om ett föreläggande kombinerat med vite inte efterföljs.²²

I december 1999 fick Elnätsutredningen (N 1999:12) i uppdrag att göra en översyn av vissa bestämmelser om nätverksamhet i ellagen. Uppdraget omfattar bl.a. att analysera gränserna för nätmyndighetens tillsynsansvar och att föreslå nödvändiga regler för att precisera detta (dir. 1999:81). I sitt delbetänkande menar Elnätsutredningen att nätmyndighetens tillsyn främst skall omfatta skäligheten av företagens avgifter och övriga villkor för överföring av el och för anslutning till en ledning eller ett ledningsnät.²³ Elnätsutredningen menar att det är tveksamt om frågan om ett nätföretag håller tillräcklig kvalitet på överföringen faller in under nätmyndighetens ansvarsområde. Utredningen påpekar att det inte finns någon uttrycklig bestämmelse som stadgar att den el som levereras skall hålla en viss kvalitet. Enligt 3 kap 9 § ellagen skall dock överföringen ske på skäligen villkor och övervakningen av denna skyldighet ingår i nätmyndighetens tillsynsansvar. Utredningen föreslår en ny bestämmelse som ålägger nätföretagen att överföra el av tillräckligt god kvalitet. Med kvalitet menar utredningen både leveranssäkerhet och spänningskvalitet. Tvister om nätägarnas skyldigheter i denna del skall prövas av nätmyndigheten efter ansökan av kunden och nätmyndighetens beslut får överklagas till allmän förvaltningsdomstol.²⁴ Med den

²¹ 12 kap ellagen (1997:857)

²² 2 kap 18 § ellagen

²³ SOU 2000:90, Elnätsföretag, Regler och tillsyn

²⁴ Utredningen redovisar också att i den finska elmarknadslagen finns regler som innebär skyldighet för nätinnehavaren att underhålla, driva och utveckla sitt nät enligt kundernas

föreslagna bestämmelsen skulle frågan om vad en tillräckligt god kvalitet skall anses innebära få lösas av praxis, t.ex. genom hänvisning till svenska och internationella standarder.²⁵ Närmare överväganden om reformbehov i fråga om leveranssäkerhet beskrivs i kapitel 12.

11.5 Utredningens principiella syn vad gäller förutsättningar för en effektiv tillsyn i säkerhetsarbetet

Som framgått av ovanstående redovisning finns ett flertal viktiga förutsättningar för att åstadkomma en effektiv tillsyn. I säkerhetsarbetet anser utredningen att det finns skäl att särskilt lyfta fram följande principer.

Utredningen menar att grunden för en effektiv tillsyn i säkerhetsarbetet är en tydlig lagstiftning. I lagstiftningen skall grundläggande säkerhetskrav på den verksamhetsansvarige fastställas

Tillsynsansvaret skall vara tydligt fördelat och reglerat. Lagstiftningen skall inte lägga fast säkerhetskrav utan att det samtidigt finns en utpekad tillsynsansvarig myndighet.

Den tillsynsansvariga myndigheten skall ha erforderlig kompetens och tillräcklig bemanning. Tillsynsorganet skall i princip vara juridiskt, ekonomiskt och administrativt oberoende i förhållande till den vars verksamhet man utövar tillsyn över.

Tillsynsorganisationen inom elområdet

Utredningen har tidigare framfört att det måste kunna ställas grundläggande säkerhetskrav för att säkra elförsörjningen i fredstid.²⁶ Därutöver menar utredningen att tillsynsansvaret på ett tydligt sätt bör kopplas till de krav som ställs i lagstiftningen.

Enligt utredningens uppfattning är dagens tillsynsorganisation på elområdet svåröverskådlig och ger ett splittrat intryck. Det finns en osäkerhet i ansvarsfördelningen mellan tillsyns-

rimliga behov och för sin del trygga kundernas tillgång av el av tillräckligt god kvalitet. Närmare bestämmelser om elkvaliteten och den tillåtna längden på elavbrotten regleras i allmänna avtalsvillkor samt i standarder för elkvaliteten som det hänvisas till i villkoren.

²⁵ Enligt Elnätsutredningen skulle en variant kunna vara att ge regeringen, eller den myndighet regeringen bestämmer, rätt att utfärda föreskrifter om vad, som enligt den generella bestämmelsen, skall anses vara godtagbar elkvalitet

²⁶ Se vidare avsnitt 3.1.2

myndigheterna angående tillsynsansvaret för säkerheten i elförsörjningen och det finns en risk för att vissa tillsynsfrågor inte uppmärksammas i tillräcklig grad. Som Elnätsutredningen konstaterat finns det inte någon uttrycklig bestämmelse som stadgar att den el som levereras skall hålla en viss kvalitet med avseende på leveranssäkerhet och spänningskvalitet. Detta försvårar naturligtvis möjligheterna att utöva en effektiv tillsyn. Som tillsynen är organiserad idag finns även en risk för konflikter mellan tillsynsuppgifterna och de främjande och producerande uppgifter som Energimyndigheten och Svenska kraftnät har.

För att få ett samlat ansvar för tillsynen av säkerheten på elområdet föreslår utredningen att nätavdelningen inom Energimyndigheten och beredskapsfunktionen inom Svenska kraftnät frigörs från Energimyndigheten respektive Svenska kraftnät och läggs samman med Elsäkerhetsverket till en ny myndighet. Förutom att myndigheten skulle få en mer självständig och tydlig roll skulle synergieffekter uppstå genom att man kan samutnyttja teknisk och annan kompetens. Förslaget till ny tillsynsorganisation beskrivs vidare i avsnitt 13.2.3.

Tillsynsansvaret för dammsäkerhet

Det är utredningens uppfattning att länsstyrelserna har en naturlig roll som operativt tillsynsansvarig för dammsäkerhet men att det finns problem på grund av att resurserna på länsstyrelserna inte är tillräckliga för att utöva den tillsyn som erfordras. Utredningen förordar en lösning som innebär att en kvalificerad expertkompetens på dammsäkerhet står till flera länsstyrelser förfogande. Därutöver anser utredningen att det bör finnas en tydligare tillsynsvägledning för dammsäkerhet på central nivå än den främjanderoll som Svenska kraftnät har idag. Den centrala tillsynsfunktionen bör omfatta såväl kraftverksdammar som dammar för industriändamål och kan med fördel sammanföras med den nya tillsynsmyndighet som utredningen föreslår på elområdet.

Tillsynsorganisationen inom trafikområdet

För att säkerställa att trafikinspektionernas tillsynsuppgifter utövas självständigt gentemot verksamhetsutövaren menar utredningen att inspektionerna i princip bör vara juridiskt, ekonomiskt och

administrativt fristående i förhållande till trafikverken. Det administrativa stöd som inspektionerna erhåller från trafikverken idag kan enligt utredningens uppfattning köpas av andra myndigheter.

11.6 Sammanfattning och förslag

I detta kapitel har utredningen behandlat vissa principfrågor som gäller förutsättningar för att bedriva en effektiv tillsyn.

Utredningen framhåller betydelsen av:

Tydligt formulerade säkerhetskrav.

Ett tydligt utpekat tillsynsansvar.

Erforderlig kompetens och tillräcklig bemanning vid den tillsynsansvariga myndigheten.

Vikten av att säkerhetsaspekterna ges tillräckligt utrymme i den tillsyn som bedrivs.

Tillsynsorganets självständighet gentemot den vars verksamhet man utövar tillsyn över.

Utredningen förlär:

En ny tillsynsmyndighet bildas genom en sammanläggning av Elsäkerhetsverket, nätavdelningen vid Energimyndigheten och beredskapsfunktionen vid Svenska kraftnät.

En central tillsynsfunktion för dammsäkerhet avseende såväl kraftverksdammar som dammar för industriändamål skapas.

Kvalificerad expertkompetens på dammsäkerhet bör tillföras på länsstyrelsenivå, som kan stå till flera länsstyrelser förfogande.

Trafikinspektionerna bör i princip vara juridiskt, ekonomiskt och administrativt fristående i förhållande till trafikverken.

12 Behovet av lagändringar m.m.

12.1 Inledning

Enligt direktiven skall utredningen lämna förslag till principer för en förbättrad helhetssyn när det gäller planeringen för beredskapen mot svåra påfrestningar i fred. Med tillämpning av ansvarsprincipen skall beredskapen byggas underifrån så att samhällets basförmåga och den reguljära fredsverksamheten är utgångspunkten. Det skall prövas om funktionsbegreppet skall behållas. Vid överväganden om det är ändamålsenligt att ge någon myndighet samordnande uppgifter skall utredningen göra en avvägning mellan behovet av samordning för alla former av hot å ena sidan och behovet av särskiljande inom funktioner samt sektorer inom ramen för ett sammanhängande system å andra sidan. Om utredningen finner att det finns behov av författningsändringar skall lagtekniskt genomarbetade förslag till bestämmelser lämnas.

Några av tidigare redovisade huvudpunkter för utredningens överväganden beträffande författningsändringar är följande.

En ny grundstruktur skall kunna hantera också andra krissituationer än krig.

Grundstrukturen bör inriktas mot situationer som kräver samverkan mellan samhällsorgan inom flera olika sektorer.

Den nuvarande funktionsindelningen utgår.

Ett områdesansvar skall finnas på nationell, regional och lokal nivå, dock med en utvidgad roll för kommunerna.

Funktionsindelningen ersätts med ett planeringsansvar, ett samverkansansvar för vissa myndigheter och ett bevakningsansvar för vissa myndigheter.

Förutsättningar skapas för ett samverkansansvar som överskrider aktuella områdesgränser.

Ett nationellt krishanteringsorgan inrättas. Det skall utgöra en del av Regeringskansliet, kunna snabbt träda i funktion vid

kriser och kunna bygga på förberedande arbete utfört av en planeringsmyndighet.

Länsstyrelsernas roll vid krishantering utvecklas till förmån för en aktiv stöd- och samordningsroll i förhållande till kommunerna, framförallt under planeringsskeden men även under insatsskeden.

Särskilt viktiga åtgärder för minskad sårbarhet och ökad säkerhet är akutsjukvård som en del av skadeavhjälpare insatser och elförsörjningen som en del av den tekniska infrastrukturen.

12.2 Konstitutionella frågor

Regeringsformen ger själva ramen för hur samhället skall vara organiserat och för hur det skall fungera. I detta avsnitt anges vissa utgångspunkter som har relevans för utredningens överväganden angående behov av lagtekniska reformer. Utredningen kommenterar i avsnitten 12.3.1 och 12.3.2 hur dessa stadganden förhåller sig till det reformbehov som föreligger.

12.2.1 Normgivningen

Såväl under normala fredsförhållanden, vid krig eller krigsfara som vid svåra påfrestningar på samhället i fred gäller att den offentliga makten utövas under lagarna. Detta är den så kallade lagbundenhetens princip. Den kommunala självstyrelsen är ett centralt sätt att ge folkstyrelsen verkligt innehåll (1 kap. 1 § regeringsformen). Beslutanderätten i kommunerna skall utövas av valda församlingar (1 kap. 7 § regeringsformen).

Bestämmelser om förhållandet mellan det enskilda och det allmänna som gäller åligganden för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden, skall meddelas genom lag (8 kap. 3 § regeringsformen).

Huvuddragen av kommunernas organisation och verksamhetsformer skall bestämmas genom lag (8 kap. 5 § regeringsformen).

Riksdagen kan i lag bemyndiga regeringen att genom förordning meddela föreskrifter i en rad närmare angivna ämnen (8 kap. 7 § regeringsformen). När det gäller svåra påfrestningar på samhället i fred blir särskilt följande ämnen aktuella.

Skydd för liv, personlig säkerhet eller hälsa (p. 1),

In- eller utförelse av varor, av pengar eller av andra tillgångar, tillverkning, kommunikationer, kreditgivning, näringsverksamhet, ransonering, återanvändning och återvinning av material, utformning av byggnader, anläggningar och bebyggelsemiljö eller tillståndsplikt i fråga om åtgärder med byggnader och anläggningar (p. 3), samt
Trafik eller ordningen på allmän plats (p. 5).

Riksdagen kan vidare genom lag bemyndiga regeringen att i en förordning bestämma att föreskrifterna skall börja tillämpas (8 kap. 10 § regeringsformen). Såvitt här är aktuellt kan bemyndigandet inte gå utöver de ämnen som nämns i 7 § första stycket. Därvid kan riksdagen vidare bestämma att föreskrifter skall underställas riksdagen inom viss tid. Det kan också föreskrivas att regeringens förordning skall upphöra att gälla om underställning inte sker (8 kap. 12 § regeringsformen).

12.2.2 Fri- och rättigheter

I regeringsformens 2 kap. anges ett antal grundläggande fri- och rättigheter. Varje enskild är tillförsäkrad bland annat mötes- och demonstrationsfrihet. Det finns också skydd mot påtvingade kroppsliga ingrepp och mot frihetsberövande (2 kap. 1 § 3–4 p, 2 kap. 6 § och 2 kap. 8 § regeringsformen). De fri- och rättigheter som anges i detta kapitel i regeringsformen har inte endast en principiell innebörd utan är rättsligen bindande.

Ett antal begränsningar av tillåtna inskränkningar i fri- och rättigheter finns i regeringsformen 2 kap. 12 § och följande paragrafer. Av särskild betydelse är att mötesfriheten och demonstrationsfriheten får begränsas av hänsyn till ordning och säkerhet vid sammankomsten eller demonstrationen eller till trafiken. I övrigt får dessa friheter begränsas endast av hänsyn till rikets säkerhet eller för att motverka farsot (2 kap. 14 § regeringsformen). I regeringsformen 2 kap. 12 § stadgas också att förslag till lag om begränsning av fri- och rättigheter kan uppskjutas på begäran av tio riksdagsledamöter.

Skydd för egendom föreskrivs i regeringsformen 2 kap. 18 §. Ingen kan tvingas avstå sin egendom till det allmänna eller till någon enskild genom expropriation eller annat sådant förfogande eller tåla att det allmänna inskränker användningen av mark eller byggnad utom när det krävs för att tillgodose angelägna allmänna

intressen. Den som tvingas avstå sin egendom skall få ersättning för förlusten. Motsvarande gäller till förmån för den för vilken det allmänna inskränker användningen av mark eller byggnad på sådant sätt att pågående markanvändning inom berörd del av fastigheten avsevärt försvåras eller skada uppkommer som är betydande i förhållande till värdet på denna del av fastigheten. Ersättning skall i samtliga fall bestämmas enligt grunder som anges i lag.

12.2.3 Regler för beredskap och krig

Lagformen kan enligt regeringsformen 13 kap. 6 § förbigås vid vissa typer av extrema situationer.

Om Sverige är i krig eller krigsfara eller om det råder sådana utomordentliga förhållanden som är föranledda av krig eller av krigsfara vari landet har befunnit sig, kan regeringen med stöd av bemyndigande i lag genom förordning meddela sådana föreskrifter i visst ämne som enligt grundlag annars skall meddelas genom lag.

Det är vidare möjligt att bemyndiga regeringen att besluta att bestämmelser avsedda för vissa extrema situationer skall börja tillämpas. Erfordras det med hänsyn till försvarsberedskapen, även i annat fall än som nämnts, kan regeringen med stöd av bemyndigande i lag genom förordning bestämma att i lag meddelad föreskrift om rekvisition eller annat sådant förfogande skall börja eller upphöra att tillämpas. I de aktuella fallen är det fråga om krig eller krigsfara, åtminstone som orsak till att utomordentliga förhållanden råder.

Det nämns alltså inte något i 13 kap. 6 § regeringsformen om de situationer där fara för Sverige saknar nära samband med krig.

I lag med bemyndigande som avses med bestämmelsen i 13 kap. 6 § regeringsformen om utökad normgivningsmakt för regeringen vid krig eller krigsfara skall det noga anges under vilka förutsättningar bemyndigandet får utnyttjas.

12.3 En generell definition av svåra påfrestningar på samhället i fred?

Försök att skapa lagstiftning för svåra påfrestningar på samhället i fred har gjorts vid olika tillfällen. Den följande redogörelsen är avsedd att ge underlag för en bedömning av vilka lagtekniska ansatser

som står till buds för att avgränsa situationer där operativ krishantering är aktuell.

12.3.1 Tidigare förslag till definitioner

Hot- och riskutredningens ansats (SOU 1995:19) var att reglera situationer med svåra påfrestningar på samhället i fred genom att föreslå en utvidgning av räddningstjänstlagen. Det skulle krävas ett särskilt beslut från regeringens sida för att sätta lagstiftningen i tillämpning. Den föreslagna lagstiftningen syftade till skydd för liv, personlig säkerhet eller hälsa. Skydd skulle fungera emot vissa händelser som utgår från delar av utredningens scenarier. Händelserna utgjorde förebilder för förutsättningar som skulle gälla för att det föreslagna nya regelverket skulle få tillämpas. Vidare hade händelserna att göra med minskning av tillgång eller ökning av efterfrågan på förnödenheter. Remisskritik framfördes emot att föreslagna åtgärder inte är räddningstjänst och att närmare rättsliga överväganden inte gjorts.

Hot- och riskutredningen utgick från att "ämnena" enligt 8 kap. 7 och 10 § regeringsformen är ett mera snävt uttryck än "syften" (SOU 1995:19 s. 194). Detta synes ha skett med utgångspunkt från framställningen hos Gustaf Petrén och Hans Ragnemalm (Sveriges Grundlagar, 12 uppl. 1980, s. 190), där begränsningen till "ämnena" betonas. Författarna tillägger dock att bemyndiganden om ikraftträdande förekommer i praktiken utan direkt lagstöd i regeringsformen, bl.a. i fråga om civillag, skattelag och processlag. De menar att detta möjligen har skett till följd av ett förbiseende hos lagstiftaren

Nils Stjernqvist och Erik Holmberg anser emellertid (Grundlagarna, 1980, s. 276) att den övergripande beteckningen "följande ämnena" används som en sammanfattande benämning på uttryck som inte är språkligt ekvivalenta, och där bl.a. p. 1 är en ändamålsbestämning men där andra uttryck under de följande punkterna stämmer bättre överens med beteckningen "ämnena". Detta talar för att begränsningen bör uppfattas avse "syften".

I departementspromemorian *Regeringens och myndigheternas befogenheter vid svåra påfrestningar på samhället* (Ds 1996:4) föreslogs att bestämmelser för svåra påfrestningar i fred skulle tas in i en särskild lag. Bestämmelserna skulle tillämpas under vissa förutsättningar utan att någon särskild åtgärd behövdes för att sätta dem i tillämpning. Förslaget hänvisade i detta sammanhang till att

en väsentlig funktion kunde falla bort. De centrala bestämmelserna i lagen avsåg åtgärder som behövs för att undvika knapphet på resurser. Dessa åtgärder i den föreslagna lagens 4-6 §§ avsåg förfoganden över egendom, tjänsteplikt och omfördelning av resurser för sjukvård.

Remisskritik framfördes mot att förutsättningarna för att tillämpa lagen var alltför oklara och mot att ersättningsfrågor inte lösts. Därvid avsågs såväl ersättning till enskilda som fördelning av kostnader mellan olika subjekt inom det allmänna. Det framhölls också att förhållandet till annan lagstiftning behövde analyseras, särskilt vad det gällde räddningstjänstlagen.

Promemoriaförslaget innehöll regler där det inte nämns något bemyndigande för regeringen eller skulle behövas någon särskild åtgärd enligt 8 kap. 7 respektive 10 §§ regeringsformen för att reglerna skulle börja tillämpas. Valet av ämnen för förfoganden i förslaget anknyter emellertid nära till delar av vad som stadgas i 8 kap. 7 § regeringsformen. Detta får tolkas så att förslaget bygger på att detta stadgande ändå skulle få betydelse. I sin tur bör detta ha förutsatt en avvägning när det gäller vilka delar av Hot- och riskutredningens scenarier som går in under tillåtna ämnen eller syften i det stadgandet.

Inget av de båda nämnda förslagen innehöll något resonemang utifrån "ordning och säkerhet" (8 kap. 7 § 1 st. 5 p. regeringsformen). En gemensam nämnare kan ha varit en avsikt att begränsa förslagen till någon form av "reparativa" åtgärder för att förslagen skulle rymmas inom området för regeringens förordningsmakt, samtidigt som man respekterar och undviker att komma i konflikt med grundläggande fri- och rättigheter.

Vissa principiella juridisk-tekniska skillnader finns mellan de två nu nämnda förslagen. Dessa är inte stora, liksom skillnader i praktiska effekter torde ha blivit begränsade. Båda utredningarna söker vidga tillämpningen av regler som redan finns. Hot- och riskutredningen önskade använda flertalet materiella bestämmelser i förfogandelagen, fastän den nya normgivningen skulle tas in i räddningstjänstlagen. Promemoriaförslaget upptog hänvisningar till andra, fredstida stadganden i räddningstjänstlagen (34 och 45 §§) där det talas om myndigheters skyldighet att bidra med personal och om ingrepp i annans rätt. Det senare förslagets hänvisningar till befintliga lagregler som skulle börja tillämpas gjordes dock på väsentliga punkter inte i lagtext utan i författningskommentar.¹

¹ Ds 1996:4 s.81-82

Promemoriaförslaget kritiserades för oklara avgränsningar mot räddningstjänstlagen. I förslaget gjordes emellertid delvis en sådan avgränsning genom att en påbörjad plikttjänstgöring enligt den lagen skulle gå före.² Andra frågor kvarstod emellertid om att beslut enligt vanlig lag kan komma att kollidera med beslut enligt normer avsedda för svåra påfrestningar i fred, t.ex. kompetenskonflikter mellan beslutande myndigheter.

Arbetsgruppen för ledningskedjan (Ds 1998:32) strävade efter att klargöra fördelning av ansvar, befogenheter, skyldigheter och resurser vid en svår påfrestning på samhället i fred. Arbetsgruppens slutsats var att en särskild definition av ett sådant tillstånd inte behövs. Därvid anförde arbetsgruppen att svåra påfrestningar i fred är ett tillstånd och att det inte behöver röra sig om händelser som inträffar plötsligt. Den föreslog att ansvarsförhållanden klargörs genom administrativa normer, där det anges att statliga och kommunala myndigheter har skyldighet att planera för extraordinära situationer. Vidare resonerade arbetsgruppen kring stödfunktioner åt regeringskansliet och förordade bland olika möjligheter att Överstyrelsen för civil beredskap skulle få en sådan funktion, dock utan att det skulle medföra något bestämmande inflytande.

Remissynpunkter framställdes från två helt skilda utgångspunkter. Ibland ifrågasätts mer eller mindre direkt om någon speciell reglering för svåra påfrestningar i fred alls behövs. Andra remissinstanser påpekar att den föreslagna utgångspunkten lämnar öppet vilka befogenheter myndigheterna skall ha i en sådan situation. Utgångspunkterna vid remissvaren över förslagen från arbetsgruppen för ledningskedjan speglade helt olika prognoser om det fredstida samhällets förmåga att hantera varje tänkbar påfrestning som är mer eller mindre möjlig att förutse.

I betänkandet Totalförsvarsplikt för det nya försvaret (SOU 2000:21) lämnade *Pliktutredningen* förslag till en lag om tjänsteplikt vid allvarliga störningar i viktiga samhällsfunktioner.

Pliktutredningens ansats är lagtekniskt i stor utsträckning den samma som promemoriaförslaget. Med allvarliga störningar i viktiga samhällsfunktioner avses omfattande avbrott inom landet i kommunikationerna eller försörjningen med livsnödvändiga förnödenheter eller tjänster om avbrottet medför allvarlig fara för många människors liv, personliga säkerhet eller hälsa. Definitionen har emellertid inte längre någon hänvisning till något enskilt av de scenarier som Hot- och riskutredningen arbetade med.

² Ds 1996:4 s. 83

Pliktutredningen återkommer emellertid till Hot- och riskutredningens ansats att särskilt nämna avbrott i kommunikationer. Metodmässigt innebär detta att man på nytt anknyter till den utredningens ansats att klargöra när en situation som innebär en svår påfrestning i fred skall anses ha inträffat, nämligen genom att ange vissa konkreta händelser som redan har inträffat. Samtidigt söker man förena detta med en annan lagteknisk ansats genom att även ta hänsyn till fara för skadliga eller farliga händelser som ännu inte har inträffat.

12.3.2 Utredningens slutsatser om teknik för lagändringar beträffande krishantering

Försöken att formulera en tydlig och allmängiltig definition av ett begrepp svåra påfrestningar på samhället i fred har som framgått mött betydande svårigheter. Begreppet har i begränsad utsträckning kommit till användning i olika lagstiftningssammanhang, nämligen i lagen (1992:1403) om totalförsvaret och höjd beredskap som en utgångspunkt för verksamhetsplanering, i elberedskapslagen (1997:288) som en faktor att beakta vid granskning av en anmälan från den som har koncession respektive i radio- och TV-lagen (1996:844) som en del av villkor för sändningstillstånd.

Olika utredningar har försökt att formulera ett allmängiltigt begrepp som en utgångspunkt för fortsatt reformarbete med krishantering. Samtliga har avstått från att framställa förslag till grundlagsändringar. När det gäller konkreta åtgärder har deras förslag väsentligen avsett reparativa åtgärder. I stor utsträckning har förslagen haft att göra med att det allmännas service till befolkningen skall kunna fungera även när den sätts på allvarliga prov, inte minst inom sjukvården.

En enhetlig definition av ett allmänt uttryck eller lagtekniskt begrepp svåra påfrestningar på samhället i fred har onekligen vissa praktiska fördelar för att skapa klarhet i diskussionen kring och lagstiftningen om samhällets hantering av kriser. Betydande svårigheter uppstår emellertid när man måste konstatera att svåra påfrestningar lika väl som en serie av enskilda händelser kan vara tillstånd, utdragna över tiden och med många och sammansatta orsaker och verkningar. En alltför abstrakt definition blir vag och leder till minskad förutsebarhet. En alltför konkret definition riskerar att inte bli heltäckande.

Ett gemensamt element i tidigare utredningars strävanden efter en generell definition synes ha varit att liv och hälsa skall skyddas i ett sådant läge. Detta överensstämmer med stadganden om regeringens förordningsmakt i regeringsformen 8 kap. 7 och 10 §§.

Stadgandenas ordalydelse ger besked om hur förordningsmakten skall vara begränsad. Mot bakgrund av de resonemang som tidigare utredningar fört om regler för hantering av fredstida påfrestningar finns det dock anledning att här söka vägledning utöver ordalagen. Enligt utredningens mening finner man här en allmän konstitutionell princip om vilka syften det är möjligt för det allmänna att tillgodose utan att grundlagsmässiga hänsyn träds för när. För detta talar också den mycket strikta uppdelning som framgår av 13 kap. regeringsformen mellan samhällets ordinära åtgärder och de förskjutningar som kan föranledas av krig eller krigsfara.

Även med ett breddat säkerhetsbegrepp och med en helhetssyn på hantering av säkerhetsfrågor över hotskalan i dess helhet finns det enligt utredningens mening inte anledning att ifrågasätta den rådande uppfattningen att krig är en i så hög grad extraordinär påfrestning att endast den motiverar en generell omställning av hur det allmännas verksamhet får och skall bedrivas.

Det vore knappast ens om man övervägde grundlagsändringar fruktbart att söka åstadkomma en allmängiltig och heltäckande lagteknisk definition för ett begrepp om svåra påfrestningar i fred. Själva uttrycket svåra påfrestningar på samhället i fred får emellertid fortsatt betydelse som en allmän orienteringspunkt för diskussionen om lösningar för samhällets krishantering. De uttryck om fredstida krishantering och liknande som används i det följande är inte avsedda att ha en sådan övergripande och allmängiltig betydelse som man tidigare eftersträvat för uttrycket svåra påfrestningar i fred.

Utredningen drar följande övergripande slutsatser om hur lagändringar bör ske.

Förändringar för en situation som i någon mening motsvarar svåra påfrestningar på samhället i fred bör göras med minsta möjliga ingrepp i det fredstida samhällets organisation i enskilda lagar som redan finns.

Någon form av särskild undantagslag bör inte komma i fråga.

Bestämmelserna bör kunna tillämpas i speciella situationer som är angivna med så stor precision som möjligt.

Det finns inte någon särskild fördel med att bestämmelserna skall börja tillämpas genom ett särskilt beslut av regeringen.

Med den valda lösningen med ändringar i begränsad omfattning i lagar som redan finns kan man uppnå att det allmännas verksamhet när rättssamhället sätts på prov fortfarande bedrivs på ett förutsebart, rättssäkert och effektivt sätt. Detta ger också uttryck för en mycket viktig demokratisk grundsats, nämligen att samhällets hantering av kriser är en normal verksamhet för att råda bot på omständigheter som inte är normala.

Utredningens uppdrag omfattar enligt direktiven i första hand att skapa ett planeringssystem för hantering av kriser i fredstid. Om lagstiftning bedöms erforderlig skall lagtekniskt genomarbetade förslag lämnas. De förslag till lagtekniska lösningar som lämnas gäller väsentligen övergripande frågor av administrativ art. I detaljfrågor där ytterligare överväganden av saklig eller politisk art är påkallade genomför utredningen resonemang om inriktningen av fortsatt lagstiftningsarbete. Detta sker även med hänsyn till att ytterligare utredningar i vissa ämnen eller detaljfrågor har aviserats.

12.4 Regler för kommuner och länsstyrelser

12.4.1 Vissa huvuddrag i den kommunala organisationen

Kommunallagen (1991:900) gäller både för kommuner och landsting. För att inte tynga framställningen när någon särskild distinktion inte behövs används i fortsättningen uttrycket "kommuner" utan att landstingen lämnas utanför resonemanget.

Kommunallagen innehåller i 2 kap. 1 § en allmän avgränsning av den kommunala kompetensen. Kommuner och landsting får själva ha hand om sådana angelägenheter av allmänt intresse som har anknytning till kommunens eller landstingets område eller deras medlemmar och som inte skall handhas enbart av staten, en annan kommun, ett annat landsting eller någon annan. I detta ligger bl.a. en *lokaliseringsprincip* såtillvida att en kommun inte får sköta en angelägenhet som ankommer enbart på en annan kommun. Enligt 2 kap. 4 § finns särskilda föreskrifter om kommunernas och landstingens befogenheter på vissa områden. Som exempel på lagar som utvidgar eller närmare bestämmer den kommunala kompetensen kan nämnas lagen (1970:663) om vissa kommunala befogenheter i fråga om sysselsättning för handikappade, lagen (1986:753) om kommunal tjänsteexport och lagen (1994:693) om rätt för kommuner och landsting att lämna internationell katastrofhjälp och annat bistånd. Även inom kommunallagens ram

förekommer bestämmelser med motsvarande syften. Kommuner har t.ex. rätt att driva näringsverksamhet under förutsättning att den inte drivs i vinstsyfte och att anställa politiska sekreterare (2 kap. 7 § och 4 kap. 30 §).

Bestämmelser om samverkan mellan kommuner finns bl.a. i fråga om gemensamma nämnder och kommunalförbund (3 kap. 3 a – 3 d §§ och 20 – 28 §§).

Om inte något annat är särskilt föreskrivet skall nämndernas verksamhetsområden och inbördes förhållanden bestämmas av fullmäktige. Vidare är det fullmäktige som beslutar i ärenden av principiell beskaffenhet eller annars av större vikt för kommunen eller landstinget, bl.a. nämndernas organisation och verksamhetsformer (3 kap. 4 § och 9 §). Fullmäktiges beslut om delegation till nämnder fattas i allmänhet en gång om året i anslutning till att budgeten fastställs. Det är också möjligt att besluta om delegation till nämnder när anslag beviljas. (Se 3 kap. 12 §.)

Föreskrifter om den kommunala organisationen under krig eller krigsfara finns i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Lagen är en beredskapslag som kan sättas i tillämpning genom beslut av regeringen. Den innehåller i 6–10 §§ bestämmelser om visst minsta antal ledamöter som erfordras för att beslut skall få fattas och om möjligheter att överflytta beslutsbefogenheter till kommunstyrelsen, till ordföranden i en nämnd eller till en eller flera andra nämnder. Förutsättningarna för detta är relativt vagt angivna med uttryck som "inte kan anstå" eller "synnerlig vikt".

Enligt lagen (1994:1720) om civilt försvar finns det en skyldighet för kommuner och landsting att vidta beredskapsförberedelser i samverkan med varandra och med statliga myndigheter. Ansvaret för förberedelserna och inriktningen av dessa ankommer i första hand på kommunstyrelsen respektive landstingsstyrelsen. Kommuner och landsting är också skyldiga att medverka i utbildning som avser beredskapsförberedelserna (se 2 kap. 1–2, 4 §§). Därutöver ansvarar kommunstyrelsen under höjd beredskap (dvs. vid krig eller krigsfara) för ledningen av den del av det civila försvaret som kommunen skall bedriva (3 kap. 1 §). Kommunstyrelsen skall också verka för att beredskapsförberedelser som berör kommunen får en enhetlig inriktning och för att samverkan kommer till stånd. Kommuner och landsting är skyldiga att lämna hjälp till andra kommuner eller landsting som har en för totalförsvaret viktig uppgift som blivit oskäligt betungande till följd av krigsskada eller

andra utomordentliga förhållanden som orsakats av krig eller krigsfara.

12.4.2 Hemställan från Svenska Kommunförbundet

Svenska Kommunförbundet har i en skrivelse till regeringen den 14 juni 1999 berört några av de kommunalrättsliga problem som kan tänkas uppkomma vid extraordinära händelser, dvs. vid andra situationer än vid höjd beredskap.

Oavsett om en sådan händelse betecknas som en svår påfrestning i fred eller som något annat kan situationen, enligt vad Kommunförbundet framhåller, ställa särskilda krav på ledning, samordning och information. Ett sätt att uppfylla stora krav på förmåga till beslut utan dröjsmål är att inrätta en krisledningsgrupp, vars beslut kan beröra flera olika nämnders verksamhetsområden.

Kommunförbundet noterar att kommunallagen inte innehåller några särskilda bestämmelser om handlingssätt vid svåra påfrestningar, utan kommunernas agerande, organisation och beslutsfattande måste i varje situation hålla sig inom kommunallagens bestämmelser. För att en krissituation skall kunna hanteras på bästa sätt är det viktigt att ingen tvekan råder beträffande en krisledningsgrupps legalitet och dess rättsliga befogenhet att fatta beslut, vilket kan göra det nödvändigt att beslutskompetens överflyttas från nämnder. En uppfattning som förekommer bland kommunerna är att beslutskompetensen bör flyttas till kommunstyrelsen. Med nuvarande utformning av kommunallagen 3 kap. 9 § är det enligt Kommunförbundet tveksamt om detta kan ske, eftersom det är kommunfullmäktige som skall besluta om nämndernas verksamhetsområden.

Utöver det som Kommunförbundet anfört bör här tilläggas att en uppfattning förekommer att kommunstyrelsen redan med nuvarande rättsläge har rätt att hantera kriser och överta befogenheter från nämnder på grund av stadgandet i 6 kap. 1 § kommunallagen. Detta innehåller att kommunstyrelsen skall leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders verksamhet. Den nyss nämnda uppfattningen framstår emellertid som mindre väl grundad med hänsyn till stadgandet i 11 kap. 7 § regeringsformen, som garanterar bl.a. kommunala nämnders självständighet genom att stadga att ingen

myndighet, inte heller riksdagen, har möjlighet att bestämma hur en förvaltningsmyndighet skall besluta i ett enskilt ärende.

Kommunförbundet hemställer i skrivelsen att regeringen vidtar de lagändringar som behövs för att kommunernas kompetens och befogenheter vid svåra påfrestningar skall klarläggas. Därvid bör enligt Kommunförbundet lagstöd införas för att kommunstyrelsen skall ges befogenhet att överta beslutanderätt från andra nämnder.

Arbete pågår inom Justitiedepartementet med direktiv till en särskild utredare för att klarlägga de frågor som förts fram av Kommunförbundet. Något beslut av regeringen om sådana direktiv föreligger ännu inte.

Kommunförbundet har i en skrift som utarbetats och utgivits i samarbete med Överstyrelsen för civil beredskap angivit fyra olika modeller för hur krishantering skall kunna ske inom en kommun. *Utskottsmodellen* bygger på inrättande av utskott enligt 6 kap. 20–22 §§ kommunallagen. Varje berörd nämnd väljer inom sig ett krisutskott. De ledamöter som utsetts utgör gemensamt en krisledningsgrupp, som emellertid inte gemensamt kan fatta beslut. Sådana fattas av varje utskott för sig, men förutsätts då ske efter gemensamma diskussioner med de andra krisutskotten inom kommunen. *Delegeringsmodellen* har en liknande innebörd. *Bråds-kandemodellen* innebär en ytterligare variant efter samma utgångspunkt genom att man beslutar om delegation enligt 6 kap. 36 § kommunallagen i ärenden som inte kan avvaktas. *Kommunstyrelsemodellen* skiljer sig från de andra modellerna på så sätt att den innebär att beslut fattas kollektivt, inte av en person med delegation. Beslut kan också fattas av en särskild krisledningsnämnd, som likaledes förutsätts kunna överta andra nämnders beslutsbefogenheter. Kommunförbundet påpekar även här att ett sådant övertagande är problematiskt med hänsyn till regeln i 3 kap. 9 § 3 p. kommunallagen, som innebär att beslut om nämnders organisation och verksamhetsformer ankommer på kommunfullmäktige.

12.4.3 Närmare om innebörden av den kommunala självstyrelsen

Frågor om den kommunala självstyrelsens närmare innebörd har behandlats av Kommittén om den kommunala självstyrelsens grundlagsskydd i betänkandet *Den kommunala självstyrelsen och grundlagen* (SOU 1996:129).

Kommittén anförde att den kommunala självstyrelsen aldrig kan vara total. Detta har på senare tid uttryckts med att kommunal självstyrelse är en grundläggande, normativ idé och princip om relationen mellan staten och kommunala organ. Bestämmande för relationens utformning anses för det första vara vilka områden inom den offentliga sektorn som skall vara statliga respektive kommunala. Ansvars- och uppgiftsfördelningen har i stor utsträckning grundats på praktiska överväganden. Den har inte reglerats i regeringsformen på annat sätt än att det föreskrivs att kommunernas åligganden och befogenheter skulle meddelas i lag. Förhållandet mellan staten och den kommunala självstyrelsen präglas av en helhetssyn där staten och kommunerna samverkar på skilda områden och i olika former för att uppnå gemensamma samhällliga mål. I förarbetena till regeringsformen ansågs att arbets- och befogenhetsfördelningen i ganska vid omfattning måste kunna ändras i takt med samhällsutvecklingen.

Kommittén drog slutsatsen att det är angeläget även för framtiden att gränserna för en kommunal självstyrelsesektor inte slås fast i grundlagen, utan i stället kan ändras i takt med den fortsatta samhällsutvecklingen. Detta hindrar emellertid inte att vissa principer för ansvars- och uppgiftsfördelningen kan komma till uttryck i regeringsformen.

I regeringsformen saknas enligt kommittén regler som säkerställer att den kommunala självstyrelsen beaktas vid normgivning. Ett sådant stadgande skulle fylla en viktig funktion och få till följd en regelmässig avvägning av självstyrelseintressena.

Kommittén föreslog närmare angivna ändringar i regeringsformen utifrån följande förslag till formulering av den kommunala självstyrelsens innebörd.

Den kommunala självstyrelsen är en grundläggande och allomfattande princip för relationen mellan stat och kommun. Den säger att kommunen respektive landstinget själv skall *styra*, dvs. besluta inom sitt område beträffande de kommunala angelägenheterna. Vilka dessa angelägenheter är bestäms genom lag. Några av dem är specialreglerade i särskild lag, och här föreligger i regel en skyldighet för kommunen eller landstinget att ombesörja dem. En förutsättning för den kommunala självstyrelsen är den kommunala beskattningsrätten. – Utmärkande för den offentliga sektorn är samverkan mellan stat och kommun. Det finns motstående intressen. Den kommunala självstyrelsen kan därför inte vara total. Frihetsgraden varierar efter angelägenheternas art. Men för folkstyrelsen representerar den kommunala självstyrelsen grundläggande värden.

Den skall därför ha en reell innebörd och väga mycket tungt i relation till de motstående intressen som kan finnas.

12.4.4 Allmänt om tänkbara styrmedel

Lagbundenhetens princip framträder på detta område när det anges i 8 kap. 5 § regeringsformen att kommunernas uppgifter skall framgå av lag.

Nämndorganisation och uppgifter skall beslutas av fullmäktige. Nuvarande kommunala samarbetsformer mellan flera kommuner utgörs av gemensamma nämnder och kommunalförbund.

När man överväger åtgärder för att hantera en kris som berör en eller flera kommuner måste inte minst tidsfaktorn beaktas noga. I en krissituation finns ofta inte tidsmässigt utrymme för vanlig beredning, vare sig för fullmäktige- eller nämndbeslut eller för etablering av samarbete mellan flera kommuner.

I praktiken har kommuner i krissituationer inrättat informella samarbets- och samordningsorgan. Likaså har kommuner tillämpat beredningsplaner för situationer som är allvarliga men inte alla har haft att göra med beredskap, något som avser krig eller krigsfara. Situationer där man lagar efter läglighet har i många lägen innehållit tydliga uttryck för den vilja till samverkan, problemlösning och improvisation som finns. Ur ett rättsligt perspektiv finns det anledning att ifrågasätta åtgärder som inte är förutsebara.

Från ett principiellt synsätt kan man i och för sig betvivla om man över huvud taget behöver ange att kommuner skall hantera kriser eller planera för krishantering. Argumentet mot att något sådant skulle vara nödvändigt är då att regeringsformen bygger på att krig och krigsfara är de enda tillstånd som är så speciella att man behöver göra någon anpassning av samhället. Till detta kommer att kommunernas uppgifter enligt lag åvilar dem i varje tänkbart läge.

På motsvarande sätt måste man närmare överväga om det i någon situation kan vara nödvändigt att överflytta ansvar eller befogenheter att fatta beslut från en nämnd till någon annan nämnd eller från en kommun till någon annan beslutsinstans. Den kommunala organisationen är emellertid mycket sammansatt och komplicerad även i mindre kommuner. Frågan är om det är realistiskt att varje nämnd i varje kommun kommer att fungera godtagbart i ett krisläge. Vidare innehåller den kommunala kompetensen bl.a. en geografisk begränsning. Det finns inte något lagstöd för att kommuner i fredstida krissituationer skulle få ägna

sig åt andra kommuners angelägenheter på ett sätt som inte är tillåtet i vanliga situationer.

12.4.5 När sätts samhällets krisåtgärder på särskilda prov?

Som redan berörts bör lösningar som innebär samverkan vara huvudregel för krishantering inom och mellan kommuner. Detta bör kunna förverkligas genom att kommunerna fortsätter att sluta avtal för gemensam krishantering. Emellertid är detta inte tillräckligt som beredskap för svåra påfrestningar i fred, vilka kan beröra ett flertal kommuner, även i andra kombinationer än vad som förutsetts planeringsmässigt. Personer i ansvarig ställning kan ha helt olika uppfattningar om en påfrestnings omfattning och tänkbara konsekvenser. Samma sak gäller slutsatser i värderingsfrågor om i vilket avseende en påfrestning drabbar mest påtagligt eller hur prioriteringar bör göras för att den skall kunna hanteras.

När man överväger tänkbara fredstida kriser och katastrofer finns en svårighet som är en svårlöst paradox, nämligen att man försöker förutse det som man vet inte går att förutse fullt ut i alla enskildheter. Olika konstruktioner måste göras. Hot- och riskutredningen arbetade med scenarioteknik. De situationer som skisseras nedan är präglade av de scenarier som Hot- och riskutredningen formulerade. Vidare innehåller de detaljer som återgår på verkliga händelser. Inte något beskrivet förlopp gör anspråk på att göra detta i varje detalj, utan det finns ett resonerande moment. Detta utgår dock från fullt tänkbara tillspetsningar av situationer som verkligen har inträffat. Erfarenheter från olika övningar i spelform har utnyttjats. Exempelen bör betraktas som illustrationer. De skall i varierande art och grad åskådliggöra de problem som nämnts i närmast föregående stycke. Det är inte heller så att någon situation som beskrivs gör anspråk på att vara av en sådan dignitet att den skulle motsvara en svår påfrestning.

En allmän iakttagelse som utredningen gjort vid studium av befintlig krisplanering och vid besök hos myndigheter är att samverkan i ett krisläge försvåras betydligt när överläggningar skall föras mellan mer än två berörda parter.

Några inslag i svårhanterade situationer kan tänkas vara följande.

Miljöfarliga ämnen används på ett riskabelt sätt i en kommun, vilket får omfattande och menliga effekter för grundvattenförsörjningen i minst en angränsande kommun.

Ett utsläpp av frätande ämnen utvecklas därhän att en utrymning i stor skala visar sig nödvändig. Förutom informationsproblem är de nyss nämnda meningsskiljaktigheterna om katastrofens omfattning och effekter för handen. Skadliga effekter uppkommer i flera kommuner. Oenighet råder om vilka effekter som inträffat, om hur de avhjälpas bäst och om vem som har bäst förutsättningar att bidra till detta.

Det sista exemplet visar klart svårigheten att förutse varje tänkbar behov. Det kan t.ex. bli fråga om ökade insatser från socialtjänsten för att ta hand om oroliga människor, behov av skollokaler för inkvartering och förläggning eller förstärkning med ytterligare förskole- och lärarpersonal som får ta hand om stora grupper av barn i förskole- och skolåldern.

Efter ett omfattande oväder uppstår oenighet mellan två länsstyrelser om var huvudansvaret för insatser på regional nivå bör ligga. Företrädare tar kontakter med en central statlig myndighet som i det aktuella läget saknar formella befogenheter att inskrida. Oenighet råder vidare mellan länsstyrelsernas företrädare och den centrala myndigheten om innebörden av kontakten. Konflikten löses slutligen sedan länsstyrelserna enats om att ledningsansvaret bör utövas där de mätbara effekterna av ovädet varit mest påtagliga.

Läckage av giftigt sediment från en industridamm tilltar snabbt. Information framförs till olika kommunala och statliga befattningshavare, av vilka inte någon anser att tänkbara skadliga effekter är av den art som faller inom vederbörandes ansvarsområde. Olika bedömningar förekommer huruvida situationen kan komma att falla inom ramen för räddningstjänst eller ej.

Som ett praktiskt exempel på svårigheten att betrakta operativ krishantering (sådan utredningen definierat denna i kapitel 5) och räddningstjänst som i huvudsak ekvivalenta kan vidare anföras diskoteksbranden i Göteborg hösten 1998. Insatsen från räddningstjänstens sida kunde avslutas efter ett par timmar. Åtgärder av olika slag och omfattning inom ramen för operativ krishantering har pågått under mycket lång tid därefter.

Det sagda belyser att situationer väl kan tänkas uppstå där samordning och informationsutbyte inte är tillräckliga medel för snabb hantering av kriser på den kommunala nivån.

Även med dessa synpunkter anser utredningen att det inte finns skäl att frångå uppfattningen att samverkan utifrån befintlig planering är det väsentligaste styrmedlet. Det finns däremot betydande vinster att göra genom att skapa förutsebarhet om vad som skall

ske när samverkan inte visar sig möjlig eller effektiv, därför att utvecklingen sker i en annan riktning eller omfattning än vad befintlig planering täcker eller därför att oenighet råder.

Redan en sådan förutsebarhet kan i praktiken bidra till att ansvarsprincipen betonas och stärks. Det blir möjligt att undvika effektivitetsförluster, missförstånd och handlingsförlamning.

12.4.6 Närmare om omfattning och utformning av reformer

Utredningens slutsatser om behovet av reformer omfattar följande frågor.

Kommunerna bör i lag åläggas att utifrån riskanalys och säkerhetsrevision planera för robusthet i utförandet av kommunala åligganden och hantering av svåra påfrestningar.

Lagstöd bör införas för att ge möjlighet att inrätta en krisorganisation med beslutsbefogenheter inom en enstaka kommun.

Ett ytterligare reformbehov kan föreligga i fråga om samordning mellan flera kommuner i situationer där förutsatt samverkan inte fungerar.

I detta sammanhang vill utredningen återkomma till vad som tidigare anförts om den kommunala självstyrelsen. Denna har inte någon absolut innebörd. Emellertid är den av central betydelse och leder till grannliga överväganden inte minst om hur maktmissbruk skall kunna förhindras. Utredningen kan inte finna att den kommunala självstyrelsen är utslagsgivande i en situation där någon utsatt kommuns situation är sådan att den kommunen inte förmår utföra sina uppgifter ensam.

När det gäller förutsättningarna för att befogenheter skall kunna överföras inom ramen för operativ krishantering inom en kommun eller ett landsting förtjänar det att erinras om vissa huvudpunkter i de försök som gjorts att definiera en svår påfrestning på samhället i fred.

Bortfall av kommunikationer

Brist på förnödenheter eller sjukvårdsresurser

Skada på person eller egendom

Fara för de olägenheter som nämnts

Anknytning till ett eller flera av Hot- och riskutredningens scenarier

Dessa försök har emellertid avsett att finna en generell definition. När det handlar om att begränsa olägenheterna av hot mot att kommuners åligganden fullgörs bör definitionen anknyta direkt till detta och till de effekter man vill undvika. Sådana kriterier kan vara följande.

Faran berör flera olika sektorer av kommunens verksamhet.

Allvarlig fara för liv, hälsa eller synnerligen omfattande materiell skada föreligger, vilket kräver insatser utöver räddningstjänst.

Tillgängliga egna resurser för att bibehålla kvaliteten i utförandet av sina uppgifter framstår som klart otillräckliga.

En situation utvecklas på ett mycket snabbt och okontrollerat sätt.

Påtagliga svårigheter föreligger att överblicka det aktuella läget.

Allvarliga hinder föreligger i möjligheter att lämna information om farans utveckling.

Tidsutdräkt skulle allvarligt försvåra möjligheter att återställa de skador som kan tänkas uppstå.

Samtidigt måste garantier mot maktmissbruk formuleras.

Det kan förtjäna att övervägas om någon särskild möjlighet till inhibition bör införas. Med de betoningar som har gjorts av samverkan som huvudregel för krishantering och om fördelning av initiativrätt och beslut ter sig en sådan möjlighet inte nödvändig utöver vad som stadgas enligt 28 § förvaltningsprocesslagen (1971:291).

12.4.7 Ändrade befogenheter inom en kommun eller mellan kommuner?

En viktig aspekt av garantier mot maktmissbruk är att ta avstånd från inslag som skulle kunna uppfattas som att den kommunala självstyrelsen, låt vara i en extrem situation där förutsatt samverkan inte fungerar, inskränks till den grad att en statlig befälsrätt skulle införas. I stället bör statens konfliktlösande roll betonas. En viktig roll kan komma att spelas av det nationella krishanteringsorgan som utredningen föreslår skall inrättas och utgöra en del av Regeringskansliet.

Hantering av kriser inom en kommun bör uppfattas som en angelägenhet som i utpräglad grad avser en kommuns rätt att styra i sina egna angelägenheter. Det skulle enligt utredningens bedöm-

ning föra alltför långt att införa någon möjlighet till beslutsrätt på den statliga eller regionala nivån när oenighet uppstår på den lokala nivån. Detta hindrar inte att särskilda överväganden är påkallade när det gäller hälso- och sjukvård. Till detta återkommer utredningen i avsnitt 12.5.

Det fallet att samverka inte är tillräcklig eller möjlig när det är två eller flera kommuner som berörs bör uppmärksammas särskilt. Om en gemensam instans inrättas för hantering kommuner emellan av krissituationer består det kommunala ansvaret och inflytandet. Man undviker också de negativa associationer som en möjlig statlig befälsrätt kan ge upphov till.

En sådan metod för gemensam kommunal krishantering skulle kunna uppfattas som att en tvistande part ges bestämmanderätt över en annan. Det förtjänar att framhållas att själva förutsebarheten om hur en tvist skall lösas i sig är ett incitament till att samverka skall fungera även i en mycket pressad situation, utan att detta leder till att en svagare part missgynnas.

Sådana ändringar i den kommunala beslutsordningen vore emellertid även i olika avseenden mera långtgående och detaljerade än vad som gäller för beredskapssituationer enligt lagen om civilt försvar. Utredningens uppdrag omfattar att se över systemet för planering för civilt försvar och svåra påfrestningar i fred. Det omfattar däremot inte att se över lagstiftningen för beredskapsförhållanden generellt, där anknytningen till krig eller krigsfara bygger på vad som stadgas i 13 kap. regeringsformen. Förslagen och det som utredningen anför om ytterligare reformbehov kan emellertid ge anledning till fortsatt översyn av beredskapslagstiftningen

Frågan är då hur man bör skapa möjligheter i kommunallagen för att lösa kriser inom en kommun och i vad mån det finns anledning att gå vidare för att skapa en gemensam ordning för hantering av kriser där flera kommuner berörs och där samverka inte är tillräcklig. Utredningen har, mot bakgrund även av de allmänna utgångspunkter för förslag till författningsändringar som redovisas i detta kapitel, slutligen stannat för att föreslå att kommunala nämnders befogenheter skall kunna överflyttas inom samma kommun. Beslutsbefogenheterna bör i ett sådant fall ankomma på kommunstyrelsen. Detta anknyter nära till den "kommunstyrelsemodell" som skisserats av Svenska Kommunförbundet. Denna modell har en mycket väsentlig fördel framför andra modeller, nämligen att beslut även i kritiska situationer med nödvändiga förenklingar fortfarande fattas gemensamt och under gemensamt ansvar, snarare än att man bygger på delegation till

enstaka beslutsfattare. En annan mycket viktig fördel som uppnås är att tvivel inte kan råda om kommunstyrelsens legitimitet som beslutsfattare i krissituationer. De tillägg som utredningen förordar beträffande 6 kap. kommunallagen är avsedda att utgöra speciallag i förhållande till fullmäktiges beslut om nämnder enligt 3 kap. 9 § kommunallagen, som då inte behöver ändras på det sätt Kommunförbundet skisserat.

Enligt utredningens mening kan erforderliga förändringar uppnås genom ändringar i kommunallagen enligt följande.

I 2 kap. kommunallagen kan klargöras kommunernas skyldighet och behörighet att planera för fredstida kriser.

Det kan då också slås fast att krishantering faller inom den kommunala kompetensen även med avseende på andra kommuner än den egna.

Kommunstyrelsen kan genom tillägg i 6 kap. kommunallagen ges möjlighet att tillfälligt ta över de befogenheter som utövas av kommunala nämnder.

Förutsättningarna för ändring av beslutsbefogenheterna bör anknytas till att allvarlig fara föreligger för att kommunen inte skall kunna fullgöra sina uppgifter enligt vad som redovisats i avsnitt 12.4.6.

Utredningen redovisar även i mera översiktlig form synpunkter kring lagändringar för att möjliggöra en gemensam kommunal krishantering. Redovisningen är avsedd särskilt att ge underlag för vidare överväganden inom ramen för den utredning om kommunalrättsliga frågor som Justitiedepartementet avser att tillsätta.

Överflyttning av ansvars- och beslutsbefogenheter skulle i extremt svåra situationer kunna ske till krisdelegerade, som utses bland personer som valts av fullmäktige i de berörda kommunerna. Detta kan enligt utredningens bedömning tillgodose regeringsformens krav på att beslutanderätten i kommuner skall utövas av valda församlingar.

En tillfällig omfördelning mellan flera kommuner för vissa mycket speciella situationer där inte krisens geografiska utbredning kunnat förutses är en mycket svår politisk bedömning. Beslutet att krisdelegerade skall träda i verksamhet bör därför ankomma på regeringen. Det är viktigt att krisdelegerades befogenheter blir rätt avpassade till den situation som är för handen. Möjligheter till begränsningar för varje enskilt fall måste

därför finnas såväl geografiskt, verksamhetsmässigt som tidsmässigt.

Ytterligare behov av lagändringar för att möjliggöra en gemensam kommunal krishantering kan tillgodoses på exempelvis följande sätt.

Bestämmelser om krisdelegerade som skall kunna utöva befogenheter i två eller flera kommuner kan införas i 3 kap. kommunallagen närmast efter vad som stadgas om gemensamma nämnder och om kommunalförbund.

Kommunerna skall i början av varje valperiod låta fullmäktige utse särskilda delegerade för operativ krishantering flera kommuner emellan.

Beslut att krisdelegerade skall träda i funktion fattas av regeringen på initiativ av en eller flera bland de kommuner som berörs.

Beslutet skall ange vilka kommuner eller nämnder inom kommuner som berörs, vilka personer bland delegerade som skall utöva befogenheterna och en tidsbegränsning, som skall kunna utvidgas.

12.4.8 Samordning mellan två län

Länsstyrelsernas uppgifter i lägen som har anknytning till situationer som innebär svåra påfrestningar på samhället i fred har framför allt att göra med räddningstjänst. Sälunda skall länsstyrelsen svara för räddningstjänsten vid utsläpp av radioaktiva ämnen från en kärnteknisk anläggning när utsläppet har en sådan omfattning att särskilda åtgärder krävs för att skydda allmänheten. Samma sak gäller vid överhängande fara för ett sådant utsläpp (se 28 § räddningstjänstlagen).

När det erfordras omfattande räddningsinsatser i kommunal räddningstjänst, skall länsstyrelsen ta över ansvaret för räddningstjänsten i de kommuner som berörs av insatserna. Om insatserna även innefattar statlig räddningstjänst skall länsstyrelsen svara för samordning av insatserna (se 34 § räddningstjänstförordningen).

Räddningstjänst i egentlig mening faller inte inom ramen för Sårbarhets- och säkerhetsutredningens uppdrag. Utredningen har tidigare utvecklat (avsnitt 5.3) att länsstyrelsens uppgifter vid fredstida kriser i första hand kommer att avse bistånd vid planering, koordinering och samordning.

Med denna inriktning gör sig behovet av reformer angående länsstyrelserna inte lika tydligt gällande som när det gäller kommunerna. Det finns emellertid anledning att uppmärksamma tänkbara situationer där länsstyrelsens bistånd till kommunerna försvåras eller hindras av oklarheter i fördelning av uppgifter i konkreta fall mellan flera länsstyrelser.

I avsnitt 12.4.7 har utredningen fört resonemang kring möjligheter att lösa tvistigheter mellan två kommuner i samband med operativ krishantering. Det som sagts där gäller i viss utsträckning även länsstyrelsernas samordnande roll. Med hänsyn till begränsningar i utredningsuppdraget och med hänsyn till frågor kring betydelsen av den kommunala självstyrelsen har utredningen avstått från att lägga fram detaljerade författningsförslag i den delen. En motsvarande ändring i länsstyrelseinstruktionen kan emellertid skisseras för det fall senare överväganden skulle ge till resultat att man behöver ge ytterligare formella bestämmelser för att lösa tvister i extrema krissituationer på lokal och regional nivå. Något av de ändringar som skisseras kan uppfattas vara inom området för befogenheter som regeringen redan har. Utredningen vill emellertid betona att betydande vinster kan göras genom ett tydliggörande av ansvar och beslutsvägar i krissituationer.

Utredningen drar följande slutsatser om tänkbara ändringar i länsstyrelseinstruktionen

Regeringen ges möjlighet att förordna att flera länsstyrelserns insatser skall ledas av en av dessa.

Förordnande får ges på initiativ av någon berörd länsstyrelse eller kommun.

Förordnande får ges när det är oundgängligen påkallat för att vidmakthålla flera länsstyrelserns stödjande eller koordinerande insatser gentemot kommuner.

12.5 Resurser för sjukvården

12.5.1 Normgivning

Hälso- och sjukvårdslagen (1982:763) innehåller ett allmänt hållet stadgande att varje landsting skall erbjuda en god hälso- och sjukvård åt dem som är bosatta inom landstinget. Även i övrigt skall landstinget verka för en god hälsa hos hela befolkningen. Behov skall ge företräde till vården (2–3 §). Varje landsting har ansvar för

dem som är bosatta inom dess område. Ansvaret gäller också personer som vistas där tillfälligt och som är i omedelbart behov av vård (3–4 §§). Planering skall ske med utgångspunkt i befolkningens behov och avse även den hälso- och sjukvård som erbjuds av privata och andra vårdgivare. Samverkan skall ske i planering och utveckling av hälso- och sjukvården med samhällsorgan, organisationer och privata vårdgivare (7–8 §§). Regeringen bemyndigas att meddela särskilda föreskrifter om hälso- och sjukvård under krig, krigsfara eller sådana utomordentliga förhållanden som är en följd av krig eller krigsfara (33 §).

12.5.2 Central ledning inom sjukvården

Socialstyrelsen är central förvaltningsmyndighet för hälso- och sjukvård. Av de formella föreskrifter som meddelats är endast ett mindre antal fortfarande i kraft. Tidigare har Socialstyrelsen utfärdat Allmänna råd, vilka emellertid successivt satts ur kraft, bl.a. Medicinsk katastrofberedskap (Allmänna råd 1992:5). Numera publicerar Socialstyrelsen motsvarande dokument under beteckningen Riktlinjer. Socialstyrelsen publicerar också ett betydande antal rapporter bl.a. i beredskapsfrågor. Vissa rapporter har en beskrivande och analyserande funktion med utgångspunkt från enskilda händelser medan andra avser central eller regional uppföljning av beredskapsfrågor. Rapporterna skall vara vägledande och kunna underlätta det arbete som bedrivs av de lokala sjukvårdshuvudmännen. Ett flertal rapporter har utgivits under en gemensam beteckning, Vårdprinciper i kris och krig, bl.a. om planeringsinriktning för katastrofsituationer.

Socialstyrelsen bedriver i samarbete med landsting och Försvarmakten ett projekt för att skapa ett datoriserat system för regional sjukvårdsledning, det s.k. IS-SWEDE-systemet. Det skall kunna samverka med andra funktioners ledningssystem, bl.a. med räddningstjänst och polis. För närvarande används det i provdrift inom fyra landsting för att stödja den vardagliga akutsjukvården. Målet är att samtliga landsting eller motsvarande skall ansluta sig till systemet inom de närmaste åren. Tekniska förutsättningar kommer då att finnas för att genomföra en central ledning av sjukvården såväl vid svåra påfrestningar i fred som vid ett väpnat angrepp.

Socialstyrelsen har vidare i mars 2000 uppmärksammat de frågor som bolagisering/privatisering och anlitande av entreprenörer in-

nebär. I en skrivelse till sjukvårdshuvudmännen sammanfattade Socialstyrelsen exempel på åtgärder för beredskapsplanering som bör regleras i avtal. Socialstyrelsen hemställde att sjukvårdshuvudmännen redovisar hur beredskapsaspekterna reglerats.

12.5.3 Bakgrund till reformbehov

Inom ramen för ordinarie organisation hanterar sjukvården s.k. vardagsolyckor. Katastrofplanering får betydelse för hantering av stora olyckor. En viss "uttunning" av den ordinarie bemanningen kan då ske för att möta det behov av vård som ett kraftigt ökat antal kirurgiska eller andra patienter föranleder. Detta innebär en viss anpassning av ordinarie organisation. I en extrem fredstida katastrofsituation, som enligt Socialstyrelsen motsvarar de lägen som brukat diskuteras under beteckningen svåra påfrestningar på samhället i fred, är det inte givet att den normala vårdstandarden kan upprätthållas genomgående utan att prioriteringar måste göras.

Under en följd av år har sjukvården genomgått omfattande strukturförändringar. Den dagliga sjukvården är inte avpassad till det resursbehov som kan uppstå i samband med svåra påfrestningar i fred. Under tiden mellan år 1995 och år 1998 begränsades möjligheten att i händelse av kris eller krig friställa vårdkapacitet inom den medicinska korttidssjukvården från omkring 30 procent till att i stort sett helt försvinna. Marginaler inom den internmedicinska verksamheten saknas i stort sett.

Multipla eller över landet utbredda katastrofer kan komma att nödvändiggöra förutom nya informations- och ledningssystem som utnyttjar modern teknik även ändrade legala förutsättningar. Svåra påfrestningar på samhället i fred har visserligen låg sannolikhet. Konsekvenserna för samhället i stort skulle kunna bli förödande om hälso- och sjukvårdsresurser inte kan utnyttjas optimalt så att patienter får en efter omständigheterna optimal vård, utan att detta försvaras av geografiska eller regionala hänsyn. Sjukvårdshuvudmännen har inte rätt enligt hälso- och sjukvårdslagen att prioritera andra delar av landet före egna behov. Detta motverkar att de själva beslutar om omfördelning av personal, resurser och patienter, särskilt i situationer där flera landsting drabbas.

Som praktiska exempel på situationer där omprioriteringar kan bli tvingande nödvändiga med mycket kort varsel kan här kortfattat hänvisas till två scenarier som utredningen har studerat.

Det första omfattar en tågurspärning med brand som följd och med mycket allvarliga brännskador hos omkring 50 personer. Det andra innebär ett terroristangrepp med biologiska stridsmedel i anslutning till allmänna kommunikationsmedel, vilket innebär en risk för att mellan 50 000 och 100 000 personer insjuknar i en livshotande sjukdom inom ett par dagar.

Exempel som de nämnda kan förefalla drastiska. Fastän de är mycket osannolika framstår de som fullt realistiska. Om sådana situationer verkligen inträffar, kommer det att uppfattas som mycket stötande att nödvändiga omprioriteringar inte kan göras. Det är angeläget att administrativa förutsättningar skapas så att de kan göras på ett ordnat och förutsebart sätt.

Den kommunala beredskapskungörelsen (1964:722) upphävdes den 1 juli 1995. Enligt 9 § hade Socialstyrelsen ett ansvar för att övervaka planläggningen av den civila hälso- och sjukvårdens samt det civila hälsoskyddets krigsorganisation. Vidare skulle Socialstyrelsen samordna rikets förberedelser för försörjning med läkemedel och sjukvårdsutrustning i krig och sörja för utbildning av sjukvårdspersonal. Socialstyrelsen skulle i krig centralt under regeringen leda den civila hälso- och sjukvården. Därvid fick Socialstyrelsen med hänsyn till behovet inom en särskild del av riket eller inom en viss verksamhetsgren av den civila hälso- och sjukvården i krig besluta om utnyttjande av vårdplatser och förflyttning av personal, patienter och förnödenheter samt i övrigt bestämma om de civila hälso- och sjukvårdsresursernas utnyttjande.

Civilbefälhavarna hade tidigare möjlighet att besluta om omfördelning av sjukvårdsresurser inom civilområdet vid höjd beredskap, 12 a § förordningen (1988:1121) med instruktion för civilbefälhavarna. Förordningen upphävdes vid ingången av år 2001 i och med att civilbefälhavarna avvecklades.

Någon motsvarande reglering finns alltså inte längre vare sig för fredstida förhållanden, beredskap eller krig.

12.5.4 Utredningens slutsatser om reformbehovet

Utredningen har i avsnitt 12.4.4 och följande utvecklat synpunkter kring tänkbara hinder för att kommunernas verksamhet i ett krisläge skall kunna utövas på det bästa sätt som över huvud taget är möjligt med hänsyn till det läge som råder. Merparten av de synpunkter som utvecklats i det nämnda avsnittet är av betydelse för

de lösningar som kan stå till buds för sjukvårdens del. De lagändringar som diskuterats där skall göra det möjligt för styrelser i kommuner eller landsting att tillfälligt ta över befogenheter från nämnder. Vid extrema fredstida kriser bör sjukvårdshuvudmännen inte heller vara begränsade till att beakta att en god sjukvård skall kunna erbjudas inom det egna geografiska området, utan även kunna beakta andra huvudmäns behov.

Till detta kommer emellertid vissa ytterligare hänsyn. När det gäller sjukvården bör det beaktas att tidspress och medborgarnas önskemål kan väntas utsätta denna för ett ovanligt intensivt tryck. Det ter sig mycket mera sannolikt här än på andra områden att en omfördelning av resurser kan komma att beröra Sverige i dess helhet. I sådana situationer skulle det inte vara godtagbart att avvakta samverkans- och förhandlingslösningar på frågor som inte har kunnat förutses i alla enskildheter.

Utredningens slutsats är att en möjlighet till fredstida omfördelning av resurser inom sjukvården vid extrema påfrestningar bör genomföras redan nu. Med hänsyn till den centrala myndighetsroll som finns hos Socialstyrelsen och att det är fråga om mycket ovanliga men ytterst allvarliga händelser bör beslut om överflyttande av förnödenheter, personal eller patienter ankomma på den myndigheten efter samråd med berörda sjukvårdshuvudmän/landsting. Regeln bör i allt väsentligt utformas efter mönster av vad som tidigare gällt enligt kommunala beredskapskungörelsen. Förutsättningarna för ett sådant beslut bör anknyta till händelser eller skaderisker av synnerligen extrem art.

Utredningen har i anslutning till resonemang om hur kommunala beslutsbefogenheter skall utövas i krislägen i avsnitt 12.4 även berört betydelsen av den kommunala självstyrelsen. När det gäller beslut om hälso- och sjukvården kan emellertid så svåra situationer uppstå att hänsynen till den kommunala självstyrelsen någon gång kan väga mindre tungt än vad som gäller för beslut i kommuner och landsting i allmänhet. För att säkerställa ett politiskt inflytande och ansvar bör beslut om ledning av hälso- och sjukvården i extrema situationer ankomma på regeringen eller den myndighet som regeringen bestämmer, närmast Socialstyrelsen.

Regeringen och Socialstyrelsen bör äläggas att samråda med berörda landsting. Samrådsskyldigheten måste gälla såväl i berednings- och beslutsskedet hos regeringen som senare i verkställandeskedet hos Socialstyrelsen.

Utredningen anser att det inte heller på detta område finns skäl att införa en särskild möjlighet till inhibition utöver vad som redan finns på förvaltningsrättens område.

När det gäller regelns form av lag eller förordning beaktar utredningen att det är fråga om en regel vars syfte är att skydda liv och hälsa. En tillämpning av det resonemang utredningen utvecklat i konstitutionella frågor i avsnitt 12.3.2 kan tala för att regeln då skulle kunna beslutas av regeringen efter bemyndigande i lag enligt regeringsformen 8 kap. 7 § utan hinder av vad som stadgas i 8 kap. 5 § om lagform för grunderna om kommunernas organisation och verksamhetsformer. En motsvarande regel för höjd beredskap finns i 33 § hälso- och sjukvårdslagen. Den tidigare regeln i 9 § kommunala beredskapskungörelsen (1964:722) tillkom år 1981, dvs. efter det att 1974 års regeringsform trätt i kraft.

Det bör emellertid också beaktas att kommunala beredskapskungörelsen ingick i ett regelverk som tillkommit tidigare. Utredningen beaktar också att hälso- och sjukvården har en helt central plats i sjukvårdshuvudmännens verksamhet. Om man ger regeringen möjlighet att besluta om formerna för att överlåta åt Socialstyrelsen att tillfälligt utöva utökade beslutsbefogenheter skulle detta kunna uppfattas som en urholkning av sjukvårdshuvudmännens inflytande och ansvar. Utredningen anser därför att det är väsentligt att det i lag klart anges under vilka förutsättningar regeringen eller den myndighet som regeringen bestämmer under extrema fredstida kriser får utöva särskilda befogenheter på hälso- och sjukvårdens område.

Förslagen innebär att möjligheter till omfördelning i fredstid kan bli större än vad som följer av beredskapslagstiftningen. Utredningens uppdrag enligt direktiven omfattar inte normgivning för höjd beredskap. Anledning kan finnas att närmare värdera detta förhållande vid en översyn av beredskapsfrågor.

Frågor kan uppkomma om hur ändringarna i kommunallagen respektive i hälso- och sjukvårdslagen skall tillämpas i förhållande till varandra. Beslut om omfördelning av resurser enligt hälso- och sjukvårdslagen kan i allmänhet komma att avse mera brådskande (ibland med behov av beslut inom sex till tolv timmar efter anmälan) och mera preciserade åtgärder än sådana som landstingens styrelser kan komma att få handlägga. Detta medför att ett beslut om omfördelning av förnödenheter, personal eller patienter enligt hälso- och sjukvårdslagen bör ha företräde.

Förslagen kan tänkas få arbetsrättsliga konsekvenser. Det är inte givet att arbetsgivares rätt att leda arbete inom sjukvården innebär

en rätt att beordra arbete på helt andra tider eller platser än vad som följer av anställnings- och kollektivavtal eller kan stämma mindre väl överens med arbetsrättslig lagstiftning. Sjukvårdshuvudmännens rätt att beordra arbetstagare till tjänstgöring eller omfattande förflyttningar är alltså inte given. När det gäller polis-tjänstgöring har man för situationer då samhället utsätts för särskilt svåra och påfrestande situationer från ordnings- och säkerhetssynpunkt förutsatt att tillgången på beredskapspoliser kan tillgodoses genom avtalslösningar (1 § förordningen, 1986:616, om beredskapspolisen). Utredningen, som även påpekar att tjänstepliktsfrågor nyligen övervägts av Pliktutredningen (SOU 2000:21), vill utan att ta ställning i frågan om tjänsteplikt dra slutsatsen att sjukvårdsarbetsmarknadens parter som ett led i huvudmännens planering för fredstida krishantering har anledning att i förhandlingar närmare överväga frågorna.

Lagändringar kan göras enligt följande.

Av de ändringar som förordats när det gäller kommunallagen följer att i ett extremt fredstida krisläge sjukvårdshuvudmännen inte är begränsade till att beakta endast det egna geografiska ansvarsområdet.

Bland målsättningsstadgandena i hälso- och sjukvårdslagen bör införas en kompletterande regel om sjukvårdshuvudmännens planering för fredstida kriser.

I ett sådant lagstiftningsärende bör närmare utvecklas att en ständigt aktuell beredskap för katastrofer, svåra påfrestningar i fred och höjd beredskap kräver en för ändamålet anpassad ledningsorganisation. Beredskapen förutsätter vidare utbildning, övning och utrustning.

I hälso- och sjukvårdslagen bör regeringen eller den myndighet regeringen bestämmer ges rätt att besluta om omfördelning av förnödenheter, personal och patienter.

Förutsättningar för att detta skall få ske bör utformas med utgångspunkt från förutsättningarna för styrelsers övertagande av befogenheter från nämnder enligt 6 kap. kommunallagen, dock med ytterligare betoning av den aktuella situationens karaktär av ett extremt krisläge.

Beslut om att Socialstyrelsen skall få utöva en sådan rätt bör i ett extremt krisläge ankomma på regeringen.

Såväl regeringen som Socialstyrelsen skall vara skyldig att kontinuerligt samråda med berörda sjukvårdshuvudmän.

12.6 Elberedskap

12.6.1 Normgivning

I ellagens (1997:857) 8 kap. finns föreskrifter om systemansvar och balansansvar. Systemansvar innebär ett övergripande ansvar för att elektriska anläggningar samverkar driftsäkert så att balans inom hela eller delar av landet kortsiktigt upprätthålls mellan produktion och förbrukning av el. Balansansvar innebär att en elleverantör bara får leverera el i uttagspunkter där någon har åtagit sig det ekonomiska ansvaret för att det nationella elsystemet tillförs lika mycket el som tas ut i uttagspunkten. Ett sådant åtagande görs genom avtal med den systemansvariga myndigheten. (Se 8 kap. 1 § och 4 §). Bestämmelser om skyddsåtgärder finns i 9 kap. I 12 kap. 1 § sägs att tillsynen över efterlevnaden av lagen och av föreskrifter eller villkor som har meddelats med stöd av lagen utövas av den eller de myndigheter regeringen bestämmer. Frågor om elsäkerhet och driftsäkerheten hos det nationella elsystemet tillses av Elsäkerhetsverket respektive Affärsverket svenska kraftnät. Dessutom utövar Statens energimyndighet tillsyn bl.a. över skäligheten av nättariffer.

I ellagen finns ett stadgande som kan få betydelse vid en svår påfrestning i fred, fastän det inte är avsett speciellt för en sådan situation. Den systemansvariga myndigheten (Svenska kraftnät) får för att upprätthålla balans mellan produktion och konsumtion av el beordra ökning eller minskning hos en producent. Detta bedöms i vissa situationer inte vara tillräckligt. Enligt 8 kap. 2 § ellagen får Svenska Kraftnät i ett sådant fall begränsa eller helt stänga av konsumtionen inom ett visst område. Denna åtgärd är av mycket drastiskt slag och har enligt uppgift aldrig tillämpats. Frånkopplingen skall ske så rättvist som möjligt, bl.a. genom att s.k. roterande belastningsfrånkoppling (RoBo) tillämpas.³ Det är därvid inte möjligt att göra någon skillnad eller prioritering mellan olika användare.

Bestämmelser om beredskap vid produktion och överföring av el samt vid handel med el finns i elberedskapslagen (1997:288), vilken reglerar bl.a. planering för elförsörjning vid höjd beredskap, men som kan få verkningar även för verksamheten i fredstid. Elberedskapsmyndigheten (Svenska kraftnät) får ålägga den som driver verksamhet enligt lagen att vidta beredskapsåtgärder. Beslutet får inte vara mer betungande än som kan anses vara skäligt med

³ Se prop. 1996/97:136 s. 74

hänsyn till anläggningens eller verksamhetens omfattning och betydelse. Svenska kraftnät skall beakta de effekter en åtgärd kan få på beredskapen inför svåra påfrestningar på samhället i fred (5 §).

Svenska kraftnät är hänvisat till att i första hand sluta avtal med producenter och har i flera sammanhang efterlyst normgivning om s.k. prioriteringsordningar.⁴ Det anses för närvarande inte vara säkert klarlagt vilka tekniska förutsättningar som finns att genomföra prioriteringar mellan enskilda användare av el. Tekniska möjligheter kan emellertid tänkas bli verklighet inom en nära framtid.

Bland Svenska kraftnäts åtgärder på avtalsmässig grund skall här nämnas en överenskommelse med Försvarsmakten den 29 augusti 2000 om stöd till elförsörjningen i fred. Svenska kraftnät har vidare den 22 december 2000 slutfört en upphandling av effektreserver, vilken innebär ökade möjligheter till eltillskott under en sträng vinter genom möjlighet att starta sju närmare angivna kraftverk. Kostnaden fördelas på de balansansvariga elföretagen.

12.6.2 Närmare om bakgrunden till nuvarande lagstiftning

Enligt det s.k. elmarknadsdirektivet (96/92/EG) skall elmarknaden i full omfattning vara konkurrensutsatt som ett viktigt steg mot fullbordande av den inre marknaden för energi. Effektiviteten vid produktion, överföring och distribution av el skall öka samtidigt som försörjningstryggheten och den europeiska ekonomins konkurrensförmåga stärks och miljöskyddet respekteras. Enligt artikel 23 i direktivet får en medlemsstat tillfälligt vidta nödvändiga skyddsåtgärder i händelse av en plötslig kris på energimarknaden om personers, anordningars eller anläggningars fysiska skydd eller säkerhet hotas eller om systemets tillstånd hotas. Åtgärderna får endast orsaka minsta möjliga störning i den inre marknads funktion och får inte vara mer omfattande än vad som är absolut nödvändigt för att avhjälpa de plötsliga svårigheter som har uppstått.

Direktivets bestämmelser om skyddsåtgärder ansågs inte behöva leda till några lagändringar när direktivet implementerades i svensk rätt.⁵

Ellagen tillkom som en del av den s.k. elmarknadsreformen. Denna innebar en avreglering av elmarknaden. Tidigare gjorde man inte någon skillnad mellan producent- och distributörsansvar. El-

⁴ Se t.ex. skr. 1998/99:33 s. 34 med hänvisning till prop. 1996/97:11 s. 53.

⁵ Prop. 1997/98:59 s. 29

marknadsreformen bygger bl.a. på att produktionen av el skall ske i konkurrens.

Genom fortsatt reformarbete har olika tänkbara konfliktsituationer reglerats. Lagändringar som trätt i kraft den 1 november 1999 innehöll att ansvaret för att det finns en balansansvarig i en elanvändares uttagpunkt flyttas över från elanvändaren till elleverantörerna (se prop. 1998/99:137). Vidare infördes regler om leveransskyldighet för samtliga elleverantörer. Leveransskyldigheten upphör endast om abonnemanget upphör, om en annan leverantör tar över leveransen eller om elanvändaren har försummat sina skyldigheter gentemot leverantören. Genom reglerna kommer det alltid att finnas en elleverantör gentemot vilken elanvändaren är betalningsansvarig.

Däremot finns det inte någon närmare reglering av hur leverans av el skall säkerställas i relationen mellan producenter och elanvändare i stort. Det är en allvarlig brist vad gäller samhällets förmåga att via tillsyn ställa säkerhetskrav på elleverantörerna. Bakgrunden till nuvarande regel i 5 § elberedskapslagen om rätt att föreskriva beredskapsåtgärder är här av intresse. Elberedskapsutredningen (SOU 1996:149) föreslog att åtgärder skulle få föreskrivas för såväl beredskap som fredstida kriser. Ersättning skulle utgå för åtgärder som avsåg beredskap enligt ett avgiftssystem. Däremot skulle ersättning inte utgå för åtgärder som avsåg fredstida förhållanden. I propositionen (1996/97:86) begränsades regeln i 5 § elberedskapslagen, utan närmare kommentar till utredningens förslag, till att avse endast beredskapslägen. Svenska kraftnät skall emellertid beakta effekter för beredskapen mot svåra påfrestningar på samhället i fred. Ersättningssystemet för beredskapsåtgärder bygger på en avgift som tas ut av innehavare av nätkoncession.

12.6.3 Reformbehovet

Tillgången på el, leveranssäkerheten hos el och kvaliteten på den levererade elen tillhör de centrala frågor för den tekniska infrastrukturen som utredningen betraktar som absolut grundläggande för att samhället skall kunna fungera vid en svår fredstida påfrestning. Den får särskild betydelse genom att el i sin tur är en förutsättning för att andra grundläggande verksamheter och nyttigheter skall kunna fungera.

Tillgången på reserveffekt har minskat. Nu finns inte längre någon reservkapacitet, utan det är tveksamt om tillgänglig effekt

alltid är tillräcklig vinterdagar med sträng kyla. Det förtjänar vidare framhållas att bortfall av eltillförsel inom stora områden vid olika tillfällen varit mycket nära att inträffa. Under senare år har saltavlagringar fått till följd att elproduktionen och distributionen i västra Skåne varit endast några minuter från att slås ut. Till följd av att systemet bygger på redundans hade det varit en relativt långvarig och komplicerad procedur att sätta det i drift på nytt om ett avbrott verkligen hade inträffat.

Något ändrat principiellt synsätt beträffande val av styrmedel är inte nödvändigt. Ansvar för fredstida säkerhetsåtgärder är i hög grad en fråga om tillsyn och ekonomiska lösningar. Denna kan väljas utifrån olika ytterligheter som innebär finansiering från användares, det allmännas eller från producenternas sida. I det senare fallet kommer producenternas åtgärder i sista hand att bekostas genom högre elpriser. Elberedskapslagen bygger på ett mellanting i form av ett avgiftssystem. Med hänsyn till grunderna för elmarknadsreformen ter sig en lösning genom skattefinansiering långt ifrån självklar. Avgiftsfinansiering eller egenfinansiering av säkerhetsåtgärder torde i allmänhet vara att föredra.

Utredningen har i avsnitt 4 redogjort för olika principiella möjligheter när det gäller åtgärder som avser fredstida kriser. Utifrån vad som sagts där ter sig en lösning med avgiftsfinansiering godtagbar även för säkerhetsåtgärder som avser svåra påfrestningar på samhället i fred. En sådan lösning kan emellertid inte innebära att varje fredstida säkerhetsåtgärd skall finansieras avgiftsvis. Framför ett renodlat producentansvar har dock avgiftsfinansiering den fördelen att kostnadsfördelningen har utsikter att bli förutsebar och rättvis, vilket underlättar elmarknadens funktionssätt såväl under normala förhållanden som i kris. Detta får också bedömas stå i överensstämmelse med EU-rättsliga regler på området.

Med hänsyn till att elberedskapslagen i princip är en beredskapslag ter det sig vanskligt att göra det nuvarande stadgandet i 5 § elberedskapslagen direkt tillämpligt även för fredstida kris-situationer. Närmare överväganden är påkallade om hur ålägganden skall utformas för balansansvariga inom ramen för 8 kap. ellagen så att fredstida kriser skall kunna förebyggas.

I samband med bortfall av elleveranser omkring årsskiftet 2000 – 2001 har Näringsdepartementet aviserat en översyn av regelverket på detta område. Utformningen i detalj bl.a. av ett avgiftssystem bör lämpligen kunna ske inom ramen för en sådan utredning.

Det står emellertid klart att de möjligheter som står till buds för att säkerställa funktionen hos det nationella elsystemet inte är till-

räckliga eller nyanserade på det sätt som behövs för att hävda säkerhetskrav på elsystemets leveransförmåga. Uppdelningen av tillsynsfrågor på tre olika myndigheter kan också ifrågasättas. Utredningen finner mycket angeläget att kompletteringar sker bl.a. genom ändringar i 8 kap. ellagen enligt vad som anges nedan.

Utredningen föreslår följande utgångspunkter för lagändringar och fortsatta reformer

Närmare överväganden görs om möjligheter till samordning av den fredstida myndighetstillsynen på elområdet i enlighet med vad utredningen beskrivit om tillsynsfrågor i kapitel 11.

Skyldighet införs för elproducenter att vidta förberedelser för att motverka fredstida leveransbortfall av el i huvudsak enligt den ordning som ligger till grund för 5 § elberedskapslagen. Denna skyldighet samordnas med 8 kap. ellagen.

Finansiering bör ske genom ett avgiftssystem, dock inte så att varje fredstida säkerhetsåtgärd finansieras på det sättet.

Ytterligare kompletteringar görs i anslutning till nuvarande regler i 8 kap. ellagen om möjligheter att fastställa prioriteringsordningar och om att fastställa säkerhetsnivåer för produktion och leverans av el.

13 Organisatoriska konsekvenser av utredningens förslag

13.1 Utgångspunkter

I detta kapitel beskrivs de organisatoriska konsekvenserna av de förslag som utredningen har redovisat i tidigare kapitel. Med organisatoriska konsekvenser avser utredningen en förändrad myndighetsstruktur eller uppgiftsfördelning mellan olika organ.

Utredningen har redovisat principiellt hållna organisationsförslag i kapitlen 5, 7 och 11. En översikt över dessa förslag redovisas i avsnitt 13.2. Förslag som medför en förändrad myndighetsstruktur redovisas endast för den centrala nivån. På lokal och regional nivå medför utredningens förslag att kommunerna och länsstyrelserna får vidgade uppgifter i krishanteringsarbetet. Däremot behöver strukturella förändringar inte genomföras på dessa nivåer.

Grundläggande för utredningens förslag är att lokala och regionala organ ges ett ökat ansvar inom krishanteringsområdet. Resurserna för krishantering på dessa nivåer behöver därför förstärkas. Inom den centrala myndighetsorganisationen bör resurserna dock kunna minskas. Detta gäller trots att utredningen föreslår nya uppgifter och en höjd ambitionsnivå inom IT-säkerhetsområdet och vissa andra områden. En anledning till detta är att nuvarande funktionsindelning avskaffas.

De förslag som utredningen redovisar på central nivå kommer att få konsekvenser för viss personal. Detta sammanhänger med att utredningens förslag medför förändringar i myndighetsstrukturen. I det följande beskriver utredningen därför relativt detaljerat förändringarna på denna nivå. Syftet är att ge berörda myndigheter och berörd personal möjligheter att bilda sig en uppfattning om förslagets konsekvenser.

Som utredningen framhöll i kapitel 1 har utredningstiden varit kort. Den blev också kortare än avsett beroende på att utredningen inte gavs möjlighet att påbörja sitt arbete förrän i mars 2000. Detta medför att preciseringar och fortsatt utredningsarbete krävs inom

vissa områden. Vad gäller den centrala nivån föreslår utredningen att en organisationskommitté tillsätts för att organisera planeringsmyndigheten och för att bilda vissa av de IT-säkerhetsorgan som föreslås. Det bör ankomma på organisationskommittén att precisera uppgifterna för vissa organ. Utredningen behandlar genomförandefrågorna närmare i kapitel 15.

Med hänsyn till att det råder en viss osäkerhet om detaljer i utredningens organisationsförslag är det svårt att i nuvarande läge redovisa exakta uppgifter om dimensioneringen av de organ som utredningen föreslår. Mer detaljerade uppgifter om dimensioneringen bör tas fram av organisationskommittén och av de övriga organ som enligt utredningens förslag bör engageras igenomförandearbetet. Utredningen har trots detta valt att redovisa vissa bedömningar av dimensioneringen av de nya organ som föreslås. Anledningen är att man vid prövningen av utredningens förslag måste ha en grov uppfattning om dimensioneringen av dessa organ. De samlade ekonomiska konsekvenserna av utredningens förslag behandlas i kapitel 14.

13.2 Översikt över utredningens organisationsförslag

13.2.1 Organisation för krishantering

I kapitel 5 föreslog utredningen ett nytt system för hanteringen av allvarliga kriser i samhället. Med allvarliga kriser avser utredningen i första hand svåra påfrestningar på samhället i fred samt ett väpnat angrepp mot landet. Till begreppet allvarliga kriser räknar utredningen även kriser som på lokal eller regional nivå som kan uppfattas som en svår påfrestning på det regionala eller lokala samhället.

Det nya krishanteringssystemet bygger på att det skall finnas tre typer av ansvar: områdesansvar, samverkansansvar och bevakningsansvar. Områdesansvar bör finnas på nationell, regional och lokal nivå. Av störst betydelse vid hanteringen av akuta krissituationer är områdesansvaret. De organ som uppbär detta ansvar skall svara för att helhetsaspekterna beaktas såväl i en akut krissituation som i olika skeden före och efter en allvarlig krissituation. Dessa organ skall också svara för att behovet av tvärsektoriell samordning och samverkan tillgodoses.

Med *områdesansvar* avses att det på varje nivå skall finnas ett organ som har det yttersta ansvaret för att krishanteringen anpassas till de behov som finns inom det aktuella geografiska

ansvarsområdet och verkar för att de aktörer som finns inom detta område uppträder samordnat och effektivt vid hanteringen av krisen.

Med *samverkansansvar* avses att en myndighet åläggs att samverka med andra organ i syfte att tillgodose de krav på samordning och samverkan som finns inom vissa sakområden som har betydelse för hanteringen av mycket allvarliga kriser i samhället.

Med *bevakningsansvar* avses att en myndighet åläggs att genomföra de åtgärder som krävs för att tillgodose statsmakternas krav på anpassningsförmåga inför ett skärpt säkerhetspolitiskt läge och de övriga åtgärder som krävs för att upprätthålla myndighetens verksamhet vid höjd beredskap.

Utredningens förslag vad gäller samverkans- och bevakningsansvar medför att nuvarande funktionsindelning inom det civila försvaret kan avskaffas. Det är också nödvändigt att se över beredskapsförordningen och nuvarande system med beredskapsmyndigheter. Detta system bör ersättas av ett nytt system som bygger på att ett antal myndigheter tilldelas samverkans- och/eller bevakningsansvar enligt ovan.

På *nationell nivå* bör områdesansvaret utövas av regeringen med stöd av ett nationellt krishanteringsorgan. På central nivå bör också inrättas en *planeringsmyndighet* med uppgift att svara för planerings-, analys- och informationsuppgifter inom krishanteringsområdet samt att stödja det nationella krishanteringsorganet med olika typer av insatser. Utredningens förslag innebär att planeringsmyndigheten delvis tar över uppgifter som idag utförs av ÖCB och SPF. Utredningen behandlar frågor om planeringsmyndighetens uppgifter och dimensionering närmare i avsnitt 13.3.

På *regional nivå* bör områdesansvaret utövas av länsstyrelsen. Länsstyrelsens roll bör framförallt inriktas på stöd åt kommunernas krishantering samt samordning av centrala myndigheters engagemang i krisförlopp på lokal och regional nivå. Länsstyrelserna bör också ha uppföljnings-, utvärderings- och tillsynsuppgifter vad gäller den kommunala krishanteringen.

På *lokal nivå* bör områdesansvaret utövas av kommunstyrelsen. Utredningen anser att kommunernas roll vid hanteringen av allvarliga kriser i samhället bör förstärkas. Utredningen har därför föreslagit att kommunerna tilldelas ett planeringsansvar också för andra allvarliga krissituationer än höjd beredskap. Utredningen har också föreslagit förändringar av lagstiftningen vad gäller möjligheterna att inrätta särskilda krisledningsorgan inom en kommun.

Som nämnts medför det krishanteringssystem som utredningen föreslår att lokala och regionala organ ges en vidgad roll i krishantering. Detta är naturligt m h t de säkerhetspolitiska förändringar som har skett på senare år. Dessa förändringar har lett till en ökad betoning av andra allvarliga krissituationer än väpnat angrepp. Detta grundläggande synsätt medför att samspelet mellan olika nivåer i krishanteringssystemet blir ett annat än vad som har gällt inom det civila försvaret. Utredningens grundsyn medför att kommunernas roll betonas väsentligt starkare än tidigare. De förslag som utredningen redovisade i kapitel 4 om planeringssystemet är ett uttryck för detta. Ett väsentligt inslag i det nya planeringssystemet är en vidgad medverkan från kommuner och länsstyrelser i dialogen om vilka prioriteringar som bör göras i säkerhets- och beredskapsarbetet.

Utredningens förslag medför att resursförstärkningar krävs i krishanteringsorganisationen på lokal och regional nivå. Utredningen återkommer till frågor om finansieringen av dessa resursförstärkningar i kapitel 14.

13.2.2 Organisation för IT-säkerhet

Utredningen har i kapitel 7 föreslagit en rad åtgärder inom IT-säkerhetsområdet. Syftet med dessa åtgärder är att öka samhällets förmåga att förebygga, upptäcka och motverka dataintrång, virus-spridning, manipulering av information eller programvaror samt andra händelser som hotar IT-säkerheten. En särskilt allvarlig form av sådana händelser är informationsoperationer, dvs. samordnade åtgärder för att nå ekonomiska, politiska eller militära mål genom att påverka eller utnyttja en motståndares IT-system och informationen som lagras i dessa. Informationsoperationer kan också användas i rent kriminella syften.

Utredningen anser att IT-säkerheten och skyddet mot informationsoperationer är en mycket väsentlig del av arbetet med att minska sårbarheten i samhället. Som framgick av kapitlen 6 och 7 betraktar utredningen IT-system med förmåga att kommunicera med varandra som en betydelsefull del av samhällets infrastruktur. Utredningen har också påvisat att intrång via IT-system kan utgöra ett allvarligt hot mot samhällets telekommunikationer och annan IT-beroende verksamhet.

De ökade hoten mot IT-systemen är ett globalt problem som bl.a. har sin grund i den allt intensivare användningen av nätverk

med enhetliga kommunikationsprotokoll som Internet. En rad länder har vidtagit åtgärder för att möta dessa hot. Utredningens förslag har därför sin motsvarighet i åtgärder som har vidtagits eller planeras i många andra utvecklade länder.

Utredningens förslag innebär att nya IT-säkerhetsfunktioner inrättas inom vissa områden. Fyra sådana funktioner föreslås: ett övergripande samordningsorgan inom IT-säkerhetsområdet, en omvärldsanalysfunktion med inriktning på kvalificerade IT-hot, en teknikkompetensfunktion och en IT-incidenthanteringsfunktion. Dessutom föreslår utredningen att ett system för säkerhetsinriktad evaluering och certifiering av IT-produkter inrättas.

Enligt utredningens förslag bör det övergripande samordningsorganet placeras inom Regeringskansliet. Planeringsmyndigheten bör fungera som sammanhållande IT-säkerhetsmyndighet och i denna egenskap utgöra kansli åt samordningsorganet. Planeringsmyndigheten bör också svara för den omvärldsbevakning som krävs inom området.

Teknikkompetensfunktionen bör i en fristående ställning knytas till Försvarets radioanstalt (FRA). FRA är en civil myndighet som har hög kompetens inom området. IT-incidenthanteringsfunktionen bör under ett uppbyggnadsskede knytas till PTS. Funktionen bör ha en fristående ställning i förhållande till PTS. Ansvar för att bygga upp ett statligt system för säkerhetsinriktad evaluering och certifiering av IT-produkter bör läggas på Försvarets materielverk (FMV). FMV har särskild kompetens inom området teknisk evaluering.

De förslag som utredningen har redovisat medför en väsentlig ambitionshöjning inom IT-säkerhetsområdet. Ökade resurser måste därför tillföras denna verksamhet. Utredningen bedömer att de funktioner som har beskrivits ovan totalt kan komma att kräva ett resurstillskott på 35–40 årsarbetskrafter. En utökning av dessa resurser kan krävas på sikt. En del av den verksamhet som föreslås bör dock på sikt kunna finansieras med avgifter. De funktioner som planeringsmyndigheten bör svara för torde kunna begränsas till 5–10 årsarbetskrafter.

13.2.3 Tillsynsorganisationen inom elområdet

Utredningen behandlade i kapitel 11 tillsynsfrågorna på ett principiellt plan. I kapitlet redovisades också vissa förslag vad gäller tillsynsorganisationen inom elområdet. Utredningen har också före-

slagit att lagstiftningen inom detta område skall skärpas i syfte att möjliggöra en effektivare tillsyn.

Utredningens organisationsförslag innebär att Energimyndighetens nätavdelning och beredskapsfunktionen inom Svenska kraftnät frigörs från Energimyndigheten respektive Affärsverket Svenska Kraftnät och läggs samman med Elsäkerhetsverket till en ny myndighet. Den nya myndigheten bör ha ett samlat ansvar för tillsynsfrågorna inom elområdet. Den bör också fungera som central förvaltningsmyndighet för dammsäkerhetsfrågor. Utredningen kan inte se att det skulle uppstå några gräns-dragningsproblem i förhållande till annan verksamhet inom Energimyndigheten och Affärsverket svenska kraftnät. Tvärtom renodlas rollerna enligt det förslag som utredningen redovisar. Nuvarande organisation är enligt utredningens uppfattning svåröverskådlig och medför risk för att vissa tillsynsfrågor inte uppmärksammas i tillräcklig grad. I nuvarande organisation finns också risk för konflikter mellan tillsynsuppgifterna och de främjande och producerande uppgifter som Energimyndigheten och Svenska kraftnät har.

En sammanläggning av tillsynsfunktionerna borde medföra att vissa synergieffekter uppstår vid samutnyttjandet av teknisk och annan kompetens. Elsäkerhetsverket är dessutom en liten myndighet som har verksamhet på flera håll i landet. Erfarenheten visar att det är svårt att nå full effektivitet i administrationen av myndigheter som är alltför små. En samordning av tillsynsfunktionerna inom elområdet skulle medföra att bättre förutsättningar skapas för en effektiv administration av verksamheten. Den största fördelen är dock att förutsättningar skapas för en samordnad och kraftfull tillsynsverksamhet inom elområdet.

Utredningen föreslår således att en ny tillsynsmyndighet bildas genom en sammanläggning av Elsäkerhetsverket, nätavdelningen vid Energimyndigheten och beredskapsfunktionen vid Svenska kraftnät. Till den nya myndigheten bör föras befintliga tillsynsuppgifter inom elområdet samt de tillsynsuppgifter som kan bli följden av de skärpningar av ellagen som utredningen har föreslagit. Utredningen återkommer till frågor om genomförandet av förslaget i kapitel 15.

13.3 Planeringsmyndigheten

13.3.1 Uppgifter

Planeringsmyndighetens uppgifter har berörts på flera ställen i betänkandet. I det följande ges en samlad bild av de uppgifter som denna myndighet bör ha.

Planeringsmyndighetens uppgift bör vara att lämna stöd till det nationella krishanteringsorganet och till övriga organ inom krishanteringsystemet samt att svara för planerings-, samordnings-, informations- och analysuppgifter inom säkerhets- och beredskapsområdet. Planeringsmyndigheten bör också fungera som IT-säkerhetsmyndighet och i denna egenskap lämna stöd åt det IT-samordningsorgan som utredningen anser bör inrättas inom Regeringskansliet. Vidare bör planeringsmyndigheten svara för viss omvärldsanalys inom IT-säkerhetsområdet.

Planeringsmyndigheten bör ta över vissa av de uppgifter som idag utförs av ÖCB och SPF. Vidare behöver uppgiftsfördelningen mellan planeringsmyndigheten och SRV renodlas. De IT-säkerhetsuppgifter som planeringsmyndigheten tilldelas utförs inte alls idag eller är utspridda på ett stort antal organ. Utredningen återkommer till konsekvenserna för olika myndigheter längre fram i detta kapitel.

Planeringsmyndighetens uppgifter kan hänföras till följande verksamhetsområden:

- Information och ledningsstöd
- Planering och samordning
- Analys och utveckling
- Internationell verksamhet

Information och ledningsstöd

Uppgifterna inom detta område omfattar dels kansli- och sekretariatsfunktionerna för det nationella krishanteringsorganet och det övergripande samordningsorganet för IT-säkerhetsfrågor dels olika uppgifter inom informations- och ledningsstödsområdet.

Kansli- och sekretariatsfunktionerna har beskrivits relativt ingående i kapitlen 5 och 7. Anledningen till att dessa uppgifter bör läggas på planeringsmyndigheten och inte på något eller några organ inom Regeringskansliet är i första hand de kopplingar som finns mellan planeringsmyndighetens övriga uppgifter och kansli-

och sekretariatsfunktionerna. Om dessa uppgifter placerades inom Regeringskansliet finns risk för dubbelarbete och dåligt resursutnyttjande i den samlade krishanteringsorganisationen.

I övrigt bör planeringsmyndigheten ha nedanstående deluppgifter inom verksamhetsområdet information och ledningsstöd.

Metodik för beslutsfattande och samverkan vid allvarliga kriser

Krishanteringsförmåga byggs upp genom återkommande utbildning och övning. Övningar behöver regelbundet genomföras såväl i form av ledningsövningar som i form av samverkansövningar. Utveckling av scenarier och övningsmodeller bör ske på grundval av erfarenheter och faktiskt inträffade händelser. En väl genomarbetad metodik för samverkan krävs för att åstadkomma ett enhetligt uppträdande och för att kunna utnyttja alla resurser effektivt. Planeringsmyndigheten bör svara för metodutveckling inom detta område och skall förmedla de erfarenheter som förvärvas till andra aktörer i krishanteringsystemet.

Metodik för informationshantering vid allvarliga kriser

Ledning, samordning och information är uppgifter som är nära kopplade till varandra vid allvarliga krisförlopp. Inom informationsberedskapen har värdefulla erfarenheter byggts upp om hur information bör förmedlas till krisaktörer, media och allmänhet. Planeringsmyndigheten bör ha till uppgift att vidareutveckla metodiken inom detta område och att verka för att de erfarenheter som har vunnits kan nyttiggöras i akuta krissituationer.

Tekniskt ledningsstöd

Tekniskt ledningsstöd krävs för att inhämta, analysera, bearbeta och förmedla information på ett tillförlitligt och säkert sätt. En effektiv krishantering förutsätter att alla aktörer som ansvarar för ledning och samordning har tillgång till samma information samtidigt. Planeringsmyndigheten bör värdera de behov av ledningsstöd som finns inom krishanteringsystemet och samordna utvecklingen av tekniska stödsystem inom detta område.

Planering och samordning

Utredningen har i kapitel 4 skisserat huvuddragen i ett nytt planeringssystem. Systemet bygger på att planeringsinsatserna utgår från en helhetssyn som omfattar också andra allvarliga kriser på samhällsnivå än höjd beredskap. Den ekonomiska planeringsram som föreslås bör omfatta medel för alla dessa krissituationer. Planeringssystemet förutsätter också ett breddat deltagande i planeringsprocessen. Företrädare för lokala och regionala organ måste ges möjlighet att delta i och påverka processen.

Planeringsmyndigheten bör vara sammanhållande för arbetet inom det nya planeringssystemet. Detta innebär bl.a. att ett krav på samordning av det beslutsunderlag som behöver tas fram. Detta förutsätter att grundsyner och inriktningsdokument tas fram för olika områden. Utredningen har tidigare givit exempel på områden som är särskilt väsentliga från sårbarhets- och säkerhetssynpunkt.

Planeringsmyndigheten bör också svara för att förslag till fördelning av den ekonomiska planeringsramen tas fram och redovisas för regeringen. Detta måste givetvis ske i samverkan med de områdesansvariga organen på lokal och regional nivå och med myndigheter och andra organ som är verksamma inom områden som har stor betydelse från sårbarhets- och säkerhetssynpunkt. Utgångspunkten bör bl.a. vara kvalificerade risk- och sårbarhetsanalyser.

Uppföljnings- och utvärderingsinsatser bör också vara en väsentlig del av uppgifterna. Dessa insatser bör särskilt inriktas mot områden som uppfattas som särskilt väsentliga från sårbarhets- och säkerhetssynpunkt. Metodutveckling krävs för att skapa möjligheter att analysera komplexa beroendeförhållanden mellan olika system.

Planeringsmyndigheten bör ha en samordnande roll inom IT-säkerhetsområdet och vara sammanhållande för arbetet med att utveckla gemensamma strategier och riktlinjer inom detta område. Det finns en naturlig koppling mellan denna uppgift och uppgiften att fungera som kansli åt det samordningsorgan inom Regeringskansliet som utredningen har föreslagit inom IT-säkerhetsområdet.

Analys och utveckling

Kvalificerad omvärldsbevakning och omvärldsanalys inom områden som kan generera allvarliga kriser på samhällsnivå är en

nödvändig förutsättning för att skapa krishanteringsförmåga. Risk- och sårbarhetsanalyser vad gäller specifika verksamheter och system inom dessa områden bör ingå i arbetet. Denna analysverksamhet bör understödjas av forsknings- och utvecklingsinsatser inom olika områden.

Planeringsmyndighetens analysverksamhet bör bl.a. omfatta analyser av samhällsutvecklingen inom områden som är relevanta från krishanteringssynpunkt, analyser av beroendeförhållanden och sårbarhet inom områden som teknisk infrastruktur, samhällsviktiga transporter, m.m. I vissa fall kan det vara motiverat att genomföra sektorsanalyser inriktade på vissa samhällsområden, t.ex. näringslivet eller olika branscher inom detta.

Resultatet av omvärldsanalyserna bör bl.a. kunna utgöra ett ingångsvärde för planeringsprocessen. Ett annat syfte bör vara att göra det lättare för olika organ inom krishanteringssystemet att bedöma akuta situationer som kan kräva insatser. Planeringsmyndigheten bör samverka med Försvarmakten/MUST, FRA, FOI, FHS, universitet och högskolor och andra organ i syfte att bredda underlaget för analysverksamheten.

Planeringsmyndigheten bör ha till uppgift att samordna och beställa forsknings- och utvecklingsarbete inom krishanteringsområdet. Tonvikten bör läggas på forsknings- och utvecklingsinsatser som avser krishanteringsmetodik samt risk- och sårbarhetsproblem på central nivå. Inom detta område bör planeringsmyndigheten bl.a. svara för initiering av forsknings- och utvecklingsinsatser samt analys och bearbetning av forskningsresultat.

Planeringsmyndigheten bör också samordna kompetensutvecklingen för de personer som har viktiga befattningar i krishanteringssystemet. I denna uppgift bör ingå att hantera olika frågor om personalförsörjningen inom det civila försvaret.

Internationell verksamhet

Planeringsmyndigheten bör stödja det nationella krishanteringsorganet i detta organs roll som kontaktorgan för internationell samverkan inom krishanteringsområdet. Planeringsmyndigheten bör också utveckla egna kontakter med krishanteringsorgan utomlands och följa utvecklingen inom detta område. Detta förutsätter kontakter med EU, FN, NATO och andra internationella organisationer. Det är dock väsentligt att myndighetens internationella

kontaktverksamhet samordnas med de kontakter som måste hantearas på departementsnivå.

13.3.2 Dimensionering

Som nämnts anser utredningen att en organisationskommitté bör tillsättas för att genomföra vissa av de organisationsförändringar som utredningen har föreslagit. Det bör ingå i uppdraget för organisationskommittén att konkretisera planeringsmyndighetens uppgifter och att föreslå en dimensionering av verksamheten. Den dimensionering som utredningen redovisar i detta avsnitt är således preliminär.

Enligt utredningens uppfattning bör ambitionsnivån läggas högt inom de områden som planeringsmyndigheten ges ansvar för. Denna bedömning utgår från utredningens grunduppfattning att sårbarheten i samhället inom vissa områden är för hög och att det är angeläget att öka säkerheten innan samhället drabbas av en svår påfrestning i detta uttrycks egentliga bemärkelse. Utredningen uppfattar också planeringsmyndigheten som ett strategiskt verktyg för regeringen i arbetet med att förebygga sådana händelser eller förlopp.

Planeringsmyndigheten föreslås ta över vissa av de uppgifter som ÖCB och SPF har idag. Vissa uppgifter behöver också föras över från SRV till planeringsmyndigheten. I de flesta fall kommer såväl uppgifternas innehåll som sättet att arbeta med dem att förändras. Planeringsmyndigheten skall också arbeta över ett bredare krisspektra än dessa myndigheter. För vissa av de uppgifter som förs över behöver ambitionsnivån dessutom höjas väsentligt. Detta gäller bl.a. inom områden som omvärldsbevakning och omvärldsanalys, metodutveckling inom krishanteringsområdet samt uppföljning och utvärdering av genomförda insatser. Trots dessa skillnader ger den nuvarande dimensioneringen av de uppgifter som bör föras till planeringsmyndigheten en viss vägledning för dimensioneringen av planeringsmyndighetens framtida uppgifter inom detta område.

Däremot är det svårare att bedöma hur de helt nya uppgifter som tillförs planeringsmyndigheten skall dimensioneras. Enligt utredningens uppfattning bör man beträffande dessa uppgifter tillämpa en försiktighetsprincip, dvs. börja med en relativt liten bemanning för att sedan utöka om bemanningen visar sig vara otillräcklig. Generellt gäller också att den personal som planerings-

myndigheten har anledning att knyta till sig bör vara högt kvalificerad vilket medför att det kan ta tid att bemanna myndigheten.

Ytterligare en omständighet som påverkar dimensioneringen är planeringsmyndighetens möjligheter till att upphandla tjänster från andra organ. Inom delar av verksamheten torde det enligt utredningens uppfattning ligga nära till hands att ha en begränsad egen personalstyrka och istället förfoga över medel för att lägga ut uppdrag på eller köpa tjänster från forsknings- och sektorsmyndigheter, universitet och högskolor och konsultföretag.

Om man väger samman dessa omständigheter anser utredningen att c:a 100 årsarbetskrafter kan vara ett rimligt riktmärke för planeringsmyndighetens dimensionering i ett utgångsläge. Till detta kommer resurser vid den tekniska enhet som ÖCB har regeringens uppdrag att organisera. Denna verksamhet bör knytas till planeringsmyndigheten utan att ingå i planeringsmyndighetens organisation. En lämplig organisationsform kan vara att den tekniska enheten ges en relativt självständig ställning och att planeringsmyndigheten görs till chefsmyndighet för den tekniska enheten.

13.4 Översikt över utredningens organisationsförslag

13.4.1 Allmänt

I det följande redovisar utredningen konsekvenserna för den befintliga myndighetsstrukturen av de förslag som utredningen har lämnat. Framställningen begränsas till den centrala myndighetsnivån. Anledningen är att inga strukturella åtgärder krävs för att genomföra utredningens förslag på lokal och regional nivå. Konsekvenserna för kommunerna bör dessutom göras till föremål för överläggningar mellan staten och kommunerna.

Utredningen tar inte heller upp de organisatoriska konsekvenserna av att ett nationellt krishanteringsorgan och ett samordningsorgan för IT-säkerhet inrättas inom Regeringskansliet. Dessa konsekvenser torde organisatoriskt vara relativt begränsade. Utredningen begränsar sig till att konstatera att olika organisatoriska lösningar är möjliga men kommenterar inte närmare hur dessa organ bör infogas i Regeringskansliets organisation.

13.4.2 Konsekvenser för ÖCB

ÖCB är enligt sin instruktion central förvaltningsmyndighet för frågor om ledning och samordning av verksamhet inom det civila försvaret och skall även samordna den frivilliga försvarsverksamheten inom denna verksamhet. ÖCB skall i fred leda och samordna beredskapsförberedelser vid övriga funktionsansvariga myndigheter. Vidare skall myndigheten analysera och konkretisera en rad för det civila försvaret gemensamma frågor och verka för ett enhetligt uppträdande bland myndigheterna i dessa frågor. ÖCB svarar vidare för studier och planering samt för samordningen av funktionsövergripande forskning. ÖCB har under de senaste åren i olika former utvecklat stödet till de områdesansvariga organen, dvs. länsstyrelser och kommuner. ÖCB har även regeringens uppdrag att utveckla och förlägga en teknisk enhet till Sollefteå, huvudsakligen för drift och underhåll av olika tekniska system.

ÖCB är dessutom funktionsansvarig myndighet för funktionen Civil ledning (CL), Försörjning med industrivaror (IF) och Transporter (Tp).

Utredningens förslag innebär att flertalet uppgifter som ingår i den s.k. samordningsrollen förs över till planeringsmyndigheten. Uppgifternas innehåll samt arbetssättet måste dock anpassas till de nya förutsättningar som gäller för planeringsmyndigheten. Funktionerna CL, IF och Tp avvecklas enligt utredningens förslag.

Civil ledning

Huvuddelen av de samordningsuppgifter som ÖCB har inom det civila försvaret räknas till funktionen Civil ledning. Huvuddelen av dessa samordningsuppgifter överförs till planeringsmyndigheten. Även vissa uppgifter som rör utbildnings- och övningsverksamhet samt tekniskt ledningsstöd bör överföras till planeringsmyndigheten. Också vissa frågor om civil-militär samverkan samt utveckling av ledningssystem bör överföras till myndigheten.

Försörjning med industrivaror

Funktionens uppgifter vad gäller försörjning med industrivaror, beredskapslagring och försörjningsavtal med företag avvecklas. Den informationssamverkan med näringslivet som utvecklats inom ramen för ÖCB:s samordningsroll bör överföras till planerings-

myndigheten. Uppgifterna bör koncentreras till omvärldsanalyser med särskild inriktning på näringslivs-, bransch- och sårbarhetsanalyser.

Försörjningskommissionens verksamhet bör renodlas och dess roll vid hantering av försörjningskriser preciseras. Försörjningskommissionen är en renodlad beredskapsmyndighet som inte bedriver någon verksamhet i fred. Kommissionen bör administrativt knytas till planeringsmyndigheten.

Den internationella verksamheten omfattar dels samverkan med Norge och Finland genom särskilda avtal dels visst förtroendeskapande samarbete inom PFF och NATO:s Planning boards and Committees. Dessa uppgifter bör överföras till planeringsmyndigheten.

Transporter

ÖCB har inom ramen för sitt funktionsansvar inom transportområdet svarat för viss omvärldsbevakning och samordning avseende transportsektorns beredskapsförberedelser. Delar av denna verksamhet bör överföras till planeringsmyndigheten. Ett internationellt samarbete har utvecklats inom ramen för PFF och NATO:s olika transportkommittéer. Denna verksamhet bör överföras till planeringsmyndigheten.

Övrigt

Frågor som rör det civila försvarets personalförsörjning bör överföras till planeringsmyndigheten. Detta innebär att frågor som rör kontakter med frivilliga försvarsorganisationer och andra icke-statliga organisationer samt frågor som rör civilplikt bör övertas av den nya myndigheten.

De uppgifter vid ÖCB som inte förs över till planeringsmyndigheten bör enligt utredningens uppfattning avvecklas. Utredningen vill dock betona att den beskrivning som har gjorts av planeringsmyndighetens uppgifter inte är definitiv eller i alla avseenden uttömmande. Ett slutligt förslag om vilka uppgifter som planeringsmyndigheten bör ha och vilka uppgifter som bör föras över från ÖCB till planeringsmyndigheten bör utarbetas av den organisationskommitté som utredningen föreslår i kapitel 15.

13.4.3 Konsekvenser för SPF

SPF är enligt sin instruktion central förvaltningsmyndighet för det psykologiska försvaret. Myndigheten skall leda och samordna planläggningen av det psykologiska försvaret, sprida kunskap om säkerhetspolitiken och totalförsvaret samt främja och samordna andra myndigheters information inom dessa områden. Myndigheten skall också bistå andra myndigheter genom att utarbeta råd och rekommendationer för informationsverksamheten vid svåra påfrestningar på samhället i fred. SPF skall följa och analysera medieberedskapen under dessa förhållanden och lämna underlag för regeringens beslut inom detta område. I uppgifterna ingår också forskningssamordning inom verksamhetsområdet.

SPF har under senare år bidragit med värdefulla kunskaper vad gäller informationshantering under kriser och sambandet mellan denna verksamhet och lednings- och samordningsuppgifter under dessa förhållanden. Den kompetens som SPF har byggt upp inom detta område bör tas tillvara inom ramen för det nya krishanteringssystemet och inom den nya planeringsmyndigheten. SPF:s uppgifter inom detta område bör därför överföras till planeringsmyndigheten.

Planeringsmyndigheten övertar även ansvaret för de uppdrag som regeringen tidigare gett till SPF med anledning av Estonia samt har ansvar för och beredskap för eventuellt kommande regeringsuppdrag rörande Estonia.

SPF är funktionsansvarig myndighet för funktionen Psykologiskt försvar. Utredningens förslag innebär att funktionen Psykologiskt försvar avvecklas. Viss beredskapsverksamhet med inriktning på det civila försvaret bör dock kvarstå och överföras till planeringsmyndigheten. I första hand gäller detta uppgifter som har betydelse i samband med anpassningsåtgärder inför ett skärpt säkerhetspolitiskt läge.

För att säkerställa massmediaföretagens beredskapsplanering och samverkan med regeringen föreslås att en särskild Mediakommission inrättas. Denna bör organiseras som en vilande beredskapsmyndighet i fred (jfr Försörjningskommissionen). Mediakommission bör - i likhet med Försörjningskommissionen - utgöra en egen myndighet och ha en av regeringen utsedd chef. Denne bör rekryteras bland personer som har en central roll inom massmediaföretagen. Kommissionen bör dock inte bedriva någon utåtriktad verksamhet under normala förhållanden (utöver

beredskapsförberedelser). Den bör i likhet med Försörjningskommissionen administrativt knytas till planeringsmyndigheten.

De uppgifter vid SPF som inte förs över till planeringsmyndigheten bör enligt utredningens uppfattning avvecklas. Utredningen vill dock betona att den beskrivning som har gjorts av planeringsmyndighetens uppgifter inte är definitiv eller i alla avseenden uttömmande. Ett slutligt förslag om vilka uppgifter som planeringsmyndigheten bör ha och vilka uppgifter som bör föras över från SPF till planeringsmyndigheten bör utarbetas av den organisationskommitté som utredningen föreslår i kapitel 15.

13.4.4 Konsekvenser för SRV

SRV är enligt sin instruktion central förvaltningsmyndighet för frågor om olycks- och skadeförebyggande åtgärder enligt räddningstjänstlagen, landtransporter av farligt gods, anordnande av skyddsrum och skyddade utrymmen, räddningstjänst samt sanering av radioaktiva ämnen från en kärnteknisk anläggning om detta inte är en uppgift för någon annan myndighet. SRV är även central tillsynsmyndighet enligt lagen om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor. I SRV:s uppgifter ingår att samordna samhällets verksamhet för olycks- och skadeförebyggande åtgärder enligt räddningstjänstlagen samt inom räddningstjänsten. SRV har inom dessa områden angelägna uppgifter för bl.a. metod- och kompetensutveckling

SRV är funktionsansvarig myndighet för funktionen Befolkningsskydd och räddningstjänst. Utredningens förslag innebär att funktionen Befolkningsskydd och räddningstjänst avvecklas. SRV:s uppgift att svara för produktionen av platser för kommunal ledning bör överföras till planeringsmyndighetens tekniska enhet i Sollefteå. Övergripande frågor vad gäller fysiskt skydd för befolkningen bör överföras till planeringsmyndigheten. Enligt utredningens uppfattning är det väsentligt att ett enhetligt synsätt tillämpas inom det civila försvaret vad gäller fysiskt skydd. Frågor som kan lösas genom normgivning inom byggnadsområdet bör överföras till Boverket. SRV bör behålla de beredskapsuppgifter som myndigheten har vad gäller krigsräddningstjänsten.

RRV har i sin nyligen avslutade granskning av SRV¹ redovisat vissa brister i ansvarsfördelningen mellan SRV och ÖCB. Granskningen genomfördes på uppdrag av regeringen. Kommuner och

¹ Hinder för ett effektivare resursutnyttjande. RRV nr 2001:9.

länsstyrelser upplever enligt RRV de båda myndigheternas roller som oklara. Det uppges också finnas ett konkurrensförhållande mellan myndigheterna som försvårar samverkan. SRV uppges inte heller underordna sig ÖCB:s samordningsansvar inom det civila försvaret.

För egen del konstaterar utredningen att LEMO-utredningen² redan år 1993 riktade uppmärksamheten mot liknande problem. Enligt utredningens uppfattning är det angeläget att oklarheter av detta slag inte förs över till den nya organisationen. SRV:s uppgifter bör därför renodlas till att avse kompetensutveckling samt fack- och sektorsuppgifter inom de områden som SRV svarar för enligt sin instruktion. Detta kan medföra att vissa samordnings- och policyuppgifter inom riskhanteringsområdet och det internationella området bör överföras från SRV till planeringsmyndigheten. Det bör ankomma på den organisationskommitté som utredningen föreslår i kapitel 15 att närmare precisera gränssnittet mellan SRV och planeringsmyndigheten.

Utredningen har tidigare i betänkandet framhållit att kommunerna bör ges en vidgad roll i krishanteringsarbetet. Utredningen ser också ett behov av resursförstärkningar på lokal nivå för att kommunerna skall klara de nya uppgifterna. Det är därför väsentligt att utbildningen inom säkerhets- och beredskapsområdet byggs ut och anpassas bättre till kommunernas behov. Utredningen anser att SRV:s skolverksamhet med en annan inriktning och ett annat huvudmannaskap skulle kunna användas för detta ändamål. Utredningen föreslår att regeringen prövar möjligheterna att åstadkomma ett gemensamt huvudmannaskap mellan staten och kommunerna för skolverksamheten. Praktiskt skulle detta kunna ske genom att lösgöra skolverksamheten från SRV och att överlåta skolorna till ett aktiebolag som ägs gemensamt av staten och kommunerna. En sådan åtgärd skulle förbättra kommunernas inflytande över den utbildning som behövs för att kommunerna skall kunna ta på sig en vidgad roll inom krishanteringsområdet.

13.4.5 Konsekvenser för PTS, FRA och FMV

Utredningen föreslog i kapitel 7 att PTS, FRA och FMV skall ges vissa uppgifter inom IT-säkerhetsområdet. Dessa uppgifter innebär dels ett uppdrag från regeringen att organisera berörda IT-säker-

² Ansvars- och uppgiftsfördelning inom det civila försvaret. SOU 1993:95.

hetsfunktioner dels ett uppdrag att svara för driften av dessa funktioner.

PTS bör enligt utredningens förslag ges i uppdrag att organisera och driva IT-incidenthanteringsfunktionen. FRA bör ges motsvarande uppdrag vad gäller teknikkompetensfunktionen. FMV bör ges i uppdrag att organisera ett system för säkerhetsinriktad evaluering och certifiering av IT-produkter.

Berörda myndigheter bör tillföras särskilda medel för att genomföra dessa uppdrag. Det bör ankomma på respektive myndighet att förutsättningslöst pröva dimensioneringen av respektive IT-säkerhetsfunktion. Utredningens bedömning är att berörda funktioner totalt kan komma att kräva ett trettiotal årsarbetskrafter.

13.4.6 Konsekvenser för övriga myndigheter

Med övriga myndigheter avser utredningen centrala statliga myndigheter som har funktionsansvar eller beredskapsansvar enligt beredskapsförordningen (1993:242).

Utredningen föreslog i kapitel 5 att den funktionsindelning som finns inom det civila försvaret skall avvecklas. Därmed försvinner också det funktionsansvar som ett antal myndigheter inom det civila försvaret har. Funktionsansvaret medför att den funktionsansvariga myndigheten skall samordna verksamheten inom funktionen. Den funktionsansvariga myndigheten svarar också för funktionsövningar och viss annan verksamhet som är inriktad på funktionens gemensamma behov.

I det krishanteringssystem som utredningen föreslår tilldelas vissa centrala myndigheter samverkans- och/eller bevakningsansvar. Dessa åligganden bör regleras i en särskild förordning och i berörda myndigheters instruktioner. Kompletterande anvisningar kan meddelas årligen i regleringsbrev.

Samverkansansvar innebär att myndigheten skall samordna sitt arbete vad gäller allvarliga kriser med andra organ som är verksamma inom ett område som är samhällsviktigt och där det finns starka beroendeförhållanden mellan olika organs verksamhet. Bevakningsansvar innebär att myndigheten skall upprätthålla kompetens och vidtaga de övriga åtgärder som krävs för att kunna upprätthålla en verksamhet vid höjd beredskap.

Bevakningsansvaret har beröringspunkter med det beredskapsansvar som uttrycks i beredskapsförordningen men medför inte

samma långtgående krav som denna vad gäller planeringsåtgärder. Däremot bör uttryckliga krav ställas på att myndigheten skall ha anpassningsförmåga inför ett skärpt säkerhetspolitiskt läge. Utredningen anser att beredskapsansvaret bör ersättas av ett bevakningsansvar för vissa myndigheter.

Det är inte möjligt att nu redovisa en komplett lista över de myndigheter som bör ha samverkans- och/eller bevakningsansvar. Utredningen föreslår i kapitel 15 att en översyn skall genomföras av beredskapsförordningen och att en ny förordning bör tas fram. Då bör också klaras ut vilka myndigheter som bör ha samverkans- och/eller bevakningsansvar och den närmare innebörden av dessa ansvar i det enskilda fallet.

13.5 Sammanfattning och förslag

I detta kapitel har utredningen redovisat de organisatoriska konsekvenserna av de förslag som lämnats. Tonvikten har lagts på den centrala nivån. Anledningen är att förslagen på denna nivå får strukturella konsekvenser med nybildning av vissa myndigheter och nedläggning av andra som följd. Lokala och regionala organ ges vidgade uppgifter och ett vidgat ansvar. Detta förutsätter resursförstärkningar i krishanteringsorganisationen på lokal och regional nivå (kommuner och länsstyrelser).

Utredningen har föreslagit ett antal strukturella förändringar på central nivå. Inom Regeringskansliet nybildas två organ: ett nationellt krishanteringsorgan och ett samordningsorgan för IT-säkerhet. På central myndighetsnivå nybildas en planeringsmyndighet och vissa IT-säkerhetsorgan. De senare omfattar en IT-incidenthanteringsfunktion, en teknikkompetensfunktion och ett system för säkerhetsinriktad evaluering och certifiering.

Förslagen medför att ÖCB och SPF bör läggas ned. En stor del av de uppgifter som dessa myndigheter har inom planerings- och samordningsområdet respektive informationsberedskapen bör dock överföras till planeringsmyndigheten. Begränsade uppgifter kan också behöva överföras från SRV till planeringsmyndigheten.

Utredningen föreslår också att ett nytt huvudmannaskap införs för SRV:s skolverksamhet. Anledningen är att utredningens förslag förutsätter en ny inriktning av den utbildningsverksamhet som riktar sig till kommunerna och ett ökat inflytande för dessa över utbildningens inriktning.

Bildandet av planeringsmyndigheten samt nedläggningen av ÖCB och SPF frigör 50–60 årsarbetskrafter jämfört med dagens organisation. Bildandet av de IT-säkerhetsorgan som knyts till PTS, FRA och FMV kräver dock ett nytillskott om 30–35 årsarbetskrafter. Förstärkningen av länsstyrelsernas resurser inom krishanteringsområdet kan beräknas kräva ett resurstillskott på omkring 20 årsarbetskrafter. Detta innebär att de förändringar som utredningen föreslår inom den statliga myndighetsorganisationen totalt sett kan genomföras utan personalförstärkningar.

Däremot krävs ett nettotillskott av resurser till den kommunala krishanteringsverksamheten. Utredningen vill inte ange någon storlek på detta resurstillskott med hänsyn till de överläggningar som bör hållas med kommunerna. Däremot anvisar utredningen i kapitel 14 en möjlig finansieringskälla till de resurstillskott som erfordras i den kommunala krishanteringsverksamheten.

14 Ekonomiska konsekvenser av utredningens förslag

Vissa av utredningens förslag medför ökade kostnader. Det rör sig dels om de ökade satsningar på sårbarhetsreducerande åtgärder inom den tekniska infrastrukturen som utredningen föreslog i kapitel 6 dels om det nettotillskott av resurser som krävs för att kommunerna skall kunna axla sin nya roll i krishanteringssystemet. Dessutom sker en betydande omfördelning av kostnader inom den statliga myndighetsorganisationen. Bl.a. sker en minskning av kostnaderna vid de nuvarande verksamheterna vid ÖCB, SPF och SRV. Samtidigt ökar kostnaderna för IT-säkerhet, den regionala krishanteringsorganisationen och för vissa andra uppgifter.

Utredningen är angelägen om att redovisa ett förslag som är kostnadsneutralt. Utredningen vill därför anvisa möjliga finansieringskällor till de kostnadsökningar som föreslås inom vissa områden. Vad gäller den statliga myndighetsorganisationen inom de områden som berörs av utredningens förslag har detta redan gjorts i kapitel 13. Kostnaderna för myndighetsorganisationen som sådan minskar enligt utredningens förslag något trots de nya uppgifter som tillkommer. Däremot krävs resurstillskott för kommunernas satsningar inom krishanteringsområdet. Resurstillskott krävs också för att klara de ökade satsningar på sårbarhetsminskande åtgärder i den tekniska infrastrukturen som utredningen föreslår. I sammanhanget bör erinras om att utredningen i kapitel 4 har föreslagit att avgiftsfinansiering bör användas i ökad utsträckning för att bekosta säkerhetsåtgärder vad gäller den tekniska infrastrukturen.

Utredningen föreslår därför att resurstillskotten finansieras på följande sätt:

1. Omfördelning inom det civila försvarets ekonomiska planeringsram bl.a. genom minskade anslag till försörjningsberedskap och skyddsrumbyggande

2. Realisering av vissa besparingsmöjligheter i SRV:s skolverksamhet

Regeringen har i *Förändrad omvärld - omdanat försvar* (prop. 1998/99:74) gjort bedömningen att satsningar på åtgärder vad gäller försörjningsberedskapen och skyddsrummbyggnandet bör kunna minskas väsentligt. Regeringens bedömning har givetvis sin grund i det förändrade säkerhetspolitiska läget. De områden som nämns omfattar satsningar som är avsedda för höjd beredskap och som knappast bidrar till förmågan att klara fredstida kriser. Mot denna bakgrund borde medel kunna frigöras från dessa områden och tillföras de ändamål som utredningen vill främja. Dessa åtgärder bör kunna genomföras inom den ekonomiska planeringsram som nu finns avsatt för ändamål inom det civila försvaret.

RRV gör i den granskning av SRV som omnämndes i kapitel 13 bedömningen att det finns överkapacitet i SRV:s skolverksamhet. Kapacitetsutnyttjandet i denna verksamhet uppgick enligt RRV:s granskning till 60 % under år 2000. Dessutom är viss pliktutbildning enligt RRV överdimensionerad. Kostnaderna för SRV:s skolverksamhet uppgick år 2000 till 453 Mkr. Delar av verksamheten är avgiftsfinansierad. SRV förutser också en utvidgning av viss utbildning. Det underlag som RRV har redovisat visar att medel kan frigöras från SRV:s skolverksamhet genom en anpassning av produktionskapaciteten.

Utredningens slutsats är således att de nettotillskott av resurser som utredningen anser behövs inom vissa områden utan olägenheter kan finansieras genom omfördelning från vissa ändamål inom det civila försvarets ekonomiska planeringsram och genom besparingar inom SRV:s skolverksamhet. De förändringar som i övrigt sker inom den statliga myndighetsorganisationen kan finansieras genom omfördelning av förvaltningskostnader.

15 Genomförandefrågor

15.1 Utredningsarbetet

Utredningen har haft ett omfattande uppdrag. Utredningens direktiv berör flertalet av de frågor som har anknytning till beredskapen mot svåra påfrestningar på samhället i fred och verksamheten inom det civila försvaret. I utredningens uppdrag har dessutom ingått att belysa vissa IT-säkerhetsfrågor. Till detta kommer att utredningstiden har varit kort. Av olika skäl kom utredningsarbetet inte igång förrän i mars 2000. Utredningstiden har därför omfattat drygt ett år.

Den korta utredningstiden har medfört att utredningen har tvingats att prioritera mellan de arbetsuppgifter som tas upp i direktiven. Detta har inneburit att utredningen har koncentrerat sig på att skapa en grundstruktur med tillhörande styrsystem för samhällets krishantering. Grundstrukturen präglas av utredningens strävan att främja en helhetssyn på allvarliga kriser i samhället – oavsett om dessa gäller höjd beredskap eller andra allvarliga kris-situationer.

Utöver grundstrukturen har utredningen inriktat sig på att utarbeta ett relativt detaljerat förslag vad gäller IT-säkerheten. Anledningen är att dessa frågor betonas särskilt i utredningens direktiv. I den ursprungliga versionen av direktiven – juni 1999 – var avsikten att utredningen skulle redovisa ett särskilt delbetänkande i dessa frågor. Beträffande IT-frågorna har utredningen också delvis kunnat utgå från delutredningar som har gjorts av andra organ enligt särskilt uppdrag från regeringen.

Utredningen har också valt att redovisa ett relativt detaljerat förslag vad gäller andra delar av den tekniska infrastrukturen än IT-verksamhet. Främst gäller detta elförsörjningen och telekommunikationerna. Anledningen till att utredningen har behandlat dessa områden särskilt ingående är att den tekniska infrastrukturen – elförsörjningen, telekommunikationerna och

viss IT-verksamhet – enligt utredningens bedömning har en avgörande betydelse för flertalet väsentliga funktioner i det moderna samhället och för medborgarnas trygghet och säkerhet. Utredningen anser också att dessa frågor bör ges hög prioritet i det fortsatta arbetet med sårbarhets- och säkerhetsfrågorna.

Det betänkande som utredningen lägger fram innehåller av dessa skäl inte ett färdigt paket med lösningar på alla de problem som aktualiseras vid övergången till ett nytt krishanteringssystem. Kompletterande insatser behövs inom flera områden. Vidare behöver utredningens förslag samordnas med resultatet av annan pågående utredningsverksamhet, bl.a. Försvarsberedningens arbete och vissa utredningar som pågår inom Regeringskansliet. Utredningen syftar bl.a. på det utredningsarbete vad gäller Regeringskansliets krishantering som pågår inom Statsrådsberedningen samt det arbete som har genomförts inom Försvarsdepartementet vad gäller den särskilda planläggningen. Inom författningsområdet krävs samordning med resultatet av de sektorvisa genomgångar som f.n. pågår inom Regeringskansliet.

I det följande beskriver utredningen översiktligt de viktigaste inslagen i det genomförandearbete som krävs för att det nya krishanteringssystemet med stödsystem skall vara komplett. Utredningen vill betona att genomförandet kan ske stegvis och att alla detaljer inte behöver vara klara samtidigt. Tvärtom kan det vara fördelaktigt att genomföra vissa förslag vad gäller styrsystem och arbetsmetoder successivt för att på så sätt pröva sig fram och vinna erfarenheter. Enligt utredningens uppfattning är det av största vikt att man i genomförandearbetet prioriterar insatser för att sätta upp den myndighetsorganisation som utredningen har föreslagit. Då planeringsmyndigheten har organiserats kan denna dessutom ta på sig att vara den drivande kraften i det fortsatta förändringsarbetet.

15.2 Organisering av det nationella krishanteringsorganet och planeringsmyndigheten

De organisationsförslag som utredningen har redovisat medför att ÖCB och SPF läggs ned som myndigheter. En stor del av de uppgifter som ÖCB och SPF har i dag kommer att övergå till den nya planeringsmyndigheten. Uppgifternas innehåll förändras dock. Kontinuiteten med nuvarande organisation medför att det är angeläget att ta till vara den kompetens och de erfarenheter som

har byggts upp vid dessa myndigheter. Detta medför att det är väsentligt att organisationsförändringen sker snabbt för att undvika alltför stora avgångar bland berörda myndigheters personal. Av samma skäl är det väsentligt att personalen vid ÖCB och SPF på ett tidigt stadium ges tydliga besked om vilken verksamhet som kommer att bedrivas i den nya planeringsmyndigheten. En viss övertalighet torde komma att uppstå bland den personal som i dag är anställd vid ÖCB och SPF.

Utredningen underströk i kapitel 13 att de förslag som utredningen redovisar i betänkandet förutsätter att SRV:s roll renodlas till att fungera som kompetens- och sektorsmyndighet inom räddningstjänstens område och inom de övriga områden som nämns i myndighetens instruktion. Med tidigare inriktning av verksamheten inom SRV finns risk stor att det konkurrensförhållande som under många år har rått mellan ÖCB och SRV kvarstår också en ny myndighetsstruktur. Utredningen har därför föreslagit att vissa policy- och samordningsuppgifter av övergripande karaktär förs över från SRV till planeringsmyndigheten. Dessa uppgifter har begränsad omfattning. Utredningen har också konstaterat att det finns anledning att överväga en förändrad inriktning och ett förändrat huvudmannaskap för SRV:s skolor. En sådan åtgärd skulle främja den vidgade roll för kommunerna i krishanteringsarbetet som utredningen eftersträvar.

Bildandet av planeringsmyndigheten är en relativt omfattande förändring. Det är därför motiverat att tillsätta en organisationskommitté med uppgift att genomföra vissa kompletterande utredningsinsatser och att sköta det praktiska arbetet med att etablera myndigheten. Utredningsuppgifterna bör bl.a. omfatta konkretisering av den nya myndighetens uppgifter och samarbetsrelationer till andra organ. De praktiska uppgifterna omfattar bl.a. utformning av den nya myndighetens organisation, bemanning av myndigheten, anskaffning av lokaler, uppbyggnad av administrativa rutiner, m.m.

Utredningen vill ånyo understryka att det är mycket väsentligt att den organisationsförändring som har föreslagits sker så snabbt som möjligt. Enligt utredningens uppfattning borde regeringen redan i höst kunna redovisa ett principförslag om att den nya planeringsmyndigheten skall inrättas. Organisationskommittén kan tillsättas så snart som riksdagen har tagit ställning till regeringens förslag. Planeringsmyndigheten kan då påbörja sitt arbete den 1 juli 2002.

Den tekniska enhet som ÖCB har fått regeringens uppdrag att organisera i Sollefteå bör knytas till planeringsmyndigheten fr.o.m. den 1 juli 2002. Planeringsmyndigheten bör vara chefsmyndighet för den tekniska enheten.

Arbetet med att organisera det nationella krishanteringsorganet bör utföras av det departement till vilket krishanteringsorganet skall knytas. Denna uppgift är mer begränsad än uppgiften att sätta upp den nya planeringsmyndigheten. Genomförandearbetet omfattar vissa kompletterande utredningsinsatser i syfte att klargöra krishanteringsorganets ställning i förhållande till andra organ inom Regeringskansliet och i förhållande till de myndigheter som kommer att engageras i organets arbete. Det kan också finnas anledning att precisera hur krishanteringsorganet skall relateras till Regeringskansliets krigsorganisation och till den krishantering vid mindre allvarliga kriser som sker inom den ordinarie departementsorganisationen. Det nationella krishanteringsorganet bör sättas upp vid samma tidpunkt som planeringsmyndigheten.

15.3 Organisering av vissa IT-säkerhetsorgan

Utredningen har föreslagit att planeringsmyndigheten skall ha ett samlat ansvar för IT-säkerhetsfrågorna på myndighetsnivå, dvs. vara IT-säkerhetsmyndighet. Planeringsmyndigheten bör också fungera som kansli åt det samordningsorgan för IT-säkerhetsfrågor som utredningen anser bör inrättas inom Regeringskansliet. Detta organ bör sättas upp av det departement som organet knyts till. Detta bör ske med inriktningen att samordningsorganet bör påbörja sin verksamhet den 1 juli 2002, dvs. vid den tidpunkt då planeringsmyndigheten och det nationella krishanteringsorganet enligt utredningens förslag etableras.

Enligt utredningens uppfattning finns det anledning att komma igång med IT-incidenthanteringsfunktionen så fort som möjligt. Regeringen bör därför uppdra åt PTS att organisera en IT-incidenthanteringsfunktion som en försöksverksamhet under en tvåårsperiod. Slutlig ställning till formerna för verksamheten och definitivt huvudmannaskap för verksamheten bör tas efter det att försöksverksamheten har avslutats. Ett regeringsuppdrag till PTS med denna innebörd bör kunna lämnas redan under förhösten 2001.

Den teknikkompetensfunktion som utredningen har föreslagit bör i en fristående form knytas till FRA. Regeringen bör därför

uppdra åt FRA att organisera en teknikkompetensfunktion med det innehåll som utredningen har föreslagit. Denna organisationsförändring bör vara genomförd senast den 1 juli 2002.

Uppgiften att bygga upp ett system för säkerhetsinriktad evaluering och certifiering bör läggas på FMV. Regeringen bör därför uppdra åt FMV att genomföra detta arbete. Arbetet bör vara slutfört senast den 1 juli 2002.

15.4 Organisering av en ny tillsynsorganisation inom elområdet

Utredningen har föreslagit att Elsäkerhetsverket, nätavdelningen inom Energimyndigheten och beredskapsfunktionen vid Svenska kraftnät (inklusive dammsäkerhetsfunktionen) skall läggas samman till en ny tillsynsmyndighet inom elområdet, med övergripande tillsynsansvar även för dammsäkerhet. En organisationskommitté bör tillsättas för att förbereda den nya myndighetens verksamhet. Detta arbete bör i tiden samordnas med den översyn av lagstiftningen inom elområdet som utredningen föreslog i kapitel 12.

15.5 Organisering av övriga delar av myndighetsstrukturen inom krishanteringsområdet

Utredningen har föreslagit att vissa centrala myndigheter skall tilldelas samverkans- och/eller bevakningsansvar. Dessa förslag medför inte några förändringar av myndighetsstrukturen inom statsförvaltningen. Det är i stället fråga om ändrade uppgifter.

Detta arbete bör kopplas till en översyn av beredskapsförordningen (1993:242). Ett första steg i arbetet bör vara att precisera begreppen samverkansansvar och bevakningsansvar och att arbeta in dessa begrepp i en ny förordning. Därefter bör man klara ut vilka myndigheter som bör ha samverkans- och/eller bevakningsansvar och vilken innebörd som dessa åtaganden bör ha i det enskilda fallet. Bestämmelser om detta bör arbetas in i respektive myndighets instruktion.

Detta arbete bör genomföras inom Regeringskansliet med något departement som sammanhållande. Arbetet bör vara slutfört den 1 juli 2002. Delar av arbetet bör slutföras i sådan tid att delresultat kan redovisas i det förslag om att inrätta planeringsmyndigheten

som regeringen enligt utredningens uppfattning bör redovisa för riksdagen under hösten 2001.

15.6 Etablering av ett nytt planeringssystem för krishantering

Utredningen har föreslagit att ett nytt planeringssystem som syftar till att minska risken för och konsekvenserna av allvarliga kriser i samhället. Grundläggande för det nya planeringssystemet bör vara att planeringen bör avse alla typer av allvarliga krissituationer och att deltagandet i den nya planeringsprocessen bör vidgas väsentligt jämfört med vad som gäller i nuvarande planeringssystem.

Arbetet med att bygga upp ett nytt planeringssystem är relativt omfattande. Följande arbetsmoment ingår:

1. Framtagning av mål för krishantering.
2. Detta arbete innebär att förslag till mål skall formuleras för krishantering. Detta bör ske i enlighet med de principer som utredningen lade fast i avsnitt 4.2. Mål bör formuleras för de samhällsområden som bedöms ha särskild betydelse från säkerhetssynpunkt samt för verksamheten inom det civila försvaret.
3. Precisering av innehållet i den ekonomiska planeringsramen.
4. Utredningen har översiktligt beskrivit vilka kostnader som bör finansieras över den ekonomiska planeringsramen. Fortsatt arbete behövs dock i syfte att avgränsa planeringsramen. Man måste också klara ut vilka anslag som skall ingå i ramen.
5. Metodutveckling avseende omvärldsbevakning samt risk- och sårbarhetsanalyser.

Utredningen har föreslagit att kvalificerade risk- och sårbarhetsanalyser med inriktning på samhällsnivån skall genomföras på lokal, regional och central nivå med respektive områdesansvarigt organ som sammanhållande. Innehållet i och formerna för dessa risk- och sårbarhetsanalyser behöver utredas närmare.

Ovanstående arbetsmoment behöver inte vara helt klara till den 1 juli 2002. Systemet bör utvecklas successivt under några år. Man får också räkna med att formerna för och innehållet i planeringsprocessen behöver tas fram stegvis. Det bör uppdras åt organisationskommittén att ta fram ett översiktligt förslag till planeringssystem till den 1 juli 2002.

En övergångsprocedur behövs för den planeringsperiod som berörs av förändringen. Det bör ankomma på organisations-

kommittén att ta fram ett förslag till hur övergången skall ske. I viss utsträckning måste arbetet bygga på underlag som utarbetas av ÖCB.

15.7 Reformerad lagstiftning inom vissa områden

Utredningen har i kapitel 12 redovisat vissa bedömningar vad gäller behovet av författningsändringar. De mest brådskande av dessa åtgärder är de författningsändringar som är en förutsättning för att den nya myndighetsorganisationen inom krishanteringsområdet skall kunna etableras. Det är också angeläget att snabbt genomföra de förslag som gäller kommunerna.

Lagstiftningsarbetet bör samordnas med de förslag som kan bli resultatet av de sektorvisa genomgångar som för närvarande genomförs inom Regeringskansliet.

15.8 Överläggningar med kommunerna om uppgifter och ersättning i det nya krishanteringssystemet

Kommunerna föreslås få vidgade uppgifter i det krishanteringssystem som utredningen har föreslagit. Nuvarande ersättningssystem avser kommunernas verksamhet inom det civila försvaret. Ett nytt ersättningssystem som beaktar de nya förutsättningarna behöver tas fram. Utformningen av detta system och storleken på ersättningen måste klaras ut i överläggningar mellan staten och kommunerna. I dessa överläggningar bör även innebörden av kommunernas nya uppgifter preciseras. Regeringen bör utse en förhandlingsman som ges till uppgift att ta upp överläggningar med Svenska kommunförbundet. Detta arbete bör påbörjas så snart som grundförutsättningarna har klarlagts.

15.9 Sammanfattning och förslag

Utredningen har i betänkandet redovisat huvuddragen i ett nytt krishanteringssystem. Betänkandet kan – vad gäller detaljeringsgraden – jämföras med den utredning som Försvarets rationaliseringsinstitut redovisade år 1984. Denna utredning bildade grund för det ledningssystem för det civila försvaret som ännu tillämpas i sina huvuddrag.

Som framgått av redovisningen i detta kapitel återstår visst arbete innan det nya krishanteringssystemet kan etableras. Enligt utredningens uppfattning bör man i det fortsatta arbetet prioritera de organisatoriska och författningsmässiga åtgärder som krävs för att sätta upp den nya myndighetsorganisationen på central nivå och de författningsändringar som krävs för att länsstyrelserna och kommunerna skall kunna ta på sig de nya uppgifter som utredningen har föreslagit.

Genomförandearbetet omfattar insatser inom bl.a. följande områden:

1. Organisering av det nationella krishanteringsorganet och planeringsmyndigheten.
2. Organisering av vissa IT-säkerhetsorgan.
3. Organisering av en ny tillsynsorganisation inom elområdet.
4. Organisering av övriga delar av myndighetsstrukturen inom krishanteringsområdet.
5. Etablering av ett nytt planeringssystem för krishanteringsarbetet.
6. Reformerad lagstiftning inom vissa områden.
7. Överläggningar med Svenska Kommunförbundet om uppgifter och ersättning för kommunerna i det nya krishanteringssystemet.

Särskilt yttrande av sakkunnige Key Hedström

Jag delar utredningens uppfattning om behovet av utveckling och reformer inom sådana områden som systemet för ledning och samordning inom det civila försvaret samt IT-säkerheten och säkerheten på elområdet.

Tyvärr, har utredningens förslag på dessa områden kompletterats med en grandios överbyggnad i form av ett nytt krishanteringssystem, som lånar sina drag från de totalförsvarsstrukturer som nu är mogna för avveckling eller redan har avvecklats. Utredningen föreslår således att ett flertal nya institutioner och begrepp introduceras i det fredsorganiserade samhället, med omfattande praktiska, organisatoriska, legala och ekonomiska konsekvenser, såväl för verksamheten inom staten, landstingen och kommunerna, som för enskilda verksamhetsutövare. Detta omfattande grepp, i kombination med den genomgående bristen på konkretion och precision i beskrivningen av såväl problem som lösningar, inger allvarliga betänkligheter. Det kan noteras, att det inte ens varit möjligt att närmare avgränsa vilka frågor och åtgärder som faller inom ramen för krishanteringssystemet.

Utredningens grundsyn reser frågan om huruvida arbetet inom det statliga politikområdet Skydd mot olyckor och inom den kommunala räddningstjänsten skall anslutas till, eller till och med underordnas, ett centralt uppritat, övergripande koncept för krishantering. Detta skulle i så fall innebära en helomvändning i fråga om den utveckling, bort från sådana koncept, som pågått under avsevärd tid inom dessa områden. Denna utveckling hör ihop med en insikt om att förmågan att förebygga och att ingripa mot olika nödlägen, allvarliga såväl som mindre allvarliga, bygger på erfarenheter från faktiskt inträffade händelser och på den förmåga till samverkan mellan berörda organ som redan finns eller håller på att utvecklas i olika delar av landet.

Det nu framlagda betänkandet kräver således att mycket viktiga principiella ställningstaganden görs. Dessutom återstår mycket arbete med att precisera förslagen och deras konsekvenser i form av nödvändig författningsreglering m.m. En av de frågor som enligt min uppfattning bör ägnas särskild uppmärksamhet i fortsättningen är hur kommunernas skyldigheter i de här berörda avseendena bör regleras. Det är därvid väsentligt att beakta de förslag som kan komma att lämnas av den särskilde utredaren för översynen av räddningstjänstlagstiftningen. För att tillgodose behoven av effektivare samordning på nationell nivå bör alternativ i form av förstärkning av olika funktioner inom Regeringskansliet prövas.

Slutligen vill jag framhålla följande med anledning av utredningens resonemang om organisatoriska konsekvenser och om förhållandet mellan den nya planeringsmyndigheten och Räddningsverket. Resonemangen är inte bara oklara utan förefaller också bygga på okunskap om sambandet mellan förebyggande, konsekvensbegränsande och skadeavhjälpande åtgärder med avseende på olyckor. Räddningsverkets roll har utvecklats av statsmakterna med betoning av detta samband. Jag anser att det är synnerligen viktigt att samhällets skydd mot olyckor fortsätter att utvecklas i huvudsak inom ramen för etablerade fredstida strukturer och inte såsom en del av ett övergripande system för civilt försvar och vissa odefinierade svåra påfrestningar på samhället i fred.

Särskilt yttrande av sakkunnige Carl Mattsson

Sårbarhets- och säkerhetsutredningen har omspant ett stort och centralt område för trygghet och säkerhet i samhället. Den har behandlat såväl principfrågor som förslag till förändrad lagstiftning. Det har skett med tidspress och med krav på förankring hos olika berörda aktörer. Utredningen tar som utgångspunkt det omfattande utredningsmaterial som utarbetats under 1990-talet liksom det arbete som bedrivits parallellt för att lägga grunden för ett reformerat försvar. Enligt min mening ger detta goda förutsättningar för att kunna lägga fram relativt långtgående förslag inom området både vad gäller principer för hantering som struktur och ansvarsfördelning.

De förslag utredning lägger fram är enligt min uppfattning väl underbyggda och avvägda. Förslagen borde dock, mot bakgrund av tillgängligt material vara mer precisa och långtgående. Det gäller inte minst lagstiftningsavsnittet avseende bl.a. kommunal ledningsorganisation vid kriser.

Utredningen tar på ett förtjänstfullt sätt upp behoven av ett bredare synsätt vad gäller sårbarhet och säkerhet. Det paras bara delvis med förslag om kompetensförstärkning hos dem som verkar inom sektorn. Detsamma gäller behovet av en utbildning för dem som söker sig till sektorn och som tillfredställer behoven i kommuner, stat och näringsliv. Det allmänna utbildningssystemet tillgodoser i dagens läge inte dessa behov.

I utredningen förs ett resonemang om att skilja ut Räddningsverket skolor och ge dem en ny huvudman. Det skapar förutsättningar för att med dessa som bas skapa nya utbildningar som tillgodoser det bredare perspektivet. Det bör också enligt min uppfattning ge en plattform för att anordna vidareutbildning av dem som verkar inom sektorn för att möta de framtida behoven. I sammanhanget är det viktigt att peka på att de framtida behoven avser såväl offentlig sektor som det privata näringslivet.

Enligt min uppfattning bör alla berörda parter inklusive näringslivet ingå i diskussionen om det framtida huvudmannaskapet liksom i utformningen av de utbildningar som skall ges vid skolorna. Förslaget att ge skolorna ett nytt huvudmannaskap har också fördelen att det skapar en breddad trovärdighet. Dessutom ger förslaget en tydligare rollfördelning mellan utbildaren och tillsynsmyndigheten för densamma. Ett alternativ till förslaget om bolagisering av skolorna med deläggande från berörda parter kan vara att inlemma dem i det allmänna skolsystemet.

Särskilt yttrande av sakkunnige Bo Riddarström

Jag står helt bakom utredarens förslag till ett nationellt krishanteringssystem baserat på områdesansvaret hos kommuner, länsstyrelser och regeringen. Detta förslag tydliggör samtidigt det politiska ansvaret för en helhetssyn på krishantering, något som en sektorsmyndighet eller sektorsorgan aldrig kan eller bör ta på sig. Förslaget innebär därmed en modernisering av synen på svensk krishantering, åtminstone upp till en nivå som redan finns i flertalet jämförbara EU-länder. För att ytterligare understyrka grundprincipen med områdesansvar borde, enligt min mening, sektorsmyndigheterna åläggas ett absolut samverkansansvar med områdesansvariga organ, således inte bara ansvar att samverka med vissa utpekade sektorsmyndigheter.

Jag delar utredarens uppfattning att säkerhet och beredskap måste byggas underifrån och att kommunerna har en nyckelroll i sammanhanget. Jag stödjer förslagen att lösa upp gränserna mellan fredsuppgifter och uppgifter vid höjd beredskap samt att tillgängliga medel skall kunna användas friare, dvs. inte bara för kompletterande åtgärder inför höjd beredskap. Utredaren har därmed förtjänstfullt visat vägen för ett krishanteringssystem som inte tar sin utgångspunkt i totalförsvaret, men som väl kan anpassas till att lösa även dessa uppgifter.

Jag anser dock att stödet till kommunerna är styvmoderligt behandlat av utredaren, särskilt frågan om länsstyrelsernas delvis nya samordnande roll gentemot kommunerna. Länsstyrelsernas mandat, dvs. ansvar, befogenheter och skyldigheter borde ha preciserats, särskilt frågan om befogenheter i skadeförebyggande situationer när räddningstjänstlagen inte kan tillämpas. Färska exempel visar att länsstyrelserna upplever sig ha oklara mandat och otillräckliga resurser för att i god tid förebygga skador t.ex. vid höga flöden. Det är inte rimligt att svensk krishantering fortfarande ska bygga på att vi ska tvingas vänta så länge att det blir fara för liv, egendom och miljö.

Länsstyrelserna har i utgångsläget mycket knappa resurser och har därmed även låg uthållighet i krissituationer. Enligt min mening är det nödvändigt att väsentligt mer resurser omfördelas till länsstyrelsernas disposition. I detta sammanhang är de föreslagna tjugotalet tjänster bara en grundplåt.

Slutligen känns det märkligt för mig att utredaren, i en sektor som årligen omsätter 2.000 miljoner kronor, ska behöva känna sig manad att i detta skede av reformarbetet föreslå en personalram för den nybildade planeringsmyndigheten. Detta ser jag som fjärran från modern mål- och resultatstyrning. Det borde rimligen ankomma på den föreslagna organisationskommittén att först konkretisera verksamhetens inriktning och omfattning. Därefter, när fördelningen av uppgifter mellan central, regional och lokal nivå har gjorts, borde det finnas underlag för ställningstagande till behovet av gemensamma stödresurser.

Särskilt yttrande av sakkunniga Ann-Louise Eksborg

Utredningens förslag innebär stora och i vissa fall principiella förändringar bl.a. vad gäller hur samhällets insatser skall samordnas och ledas vid kriser av olika slag och svårhetsgrad. Enligt min mening förs dock resonemangen som ligger till grund för förslagen genomgående på en mycket övergripande nivå. Även förslagen brister i stor utsträckning i konkretion och precision. Detta gör det svårt att värdera såväl effekterna av de föreslagna förändringarna som behovet av t.ex. författningsändringar.

Vad beträffar behovet av författningsändringar har utredningen inte haft tid att arbeta fram konkreta författningsförslag utan valt att mer skissartat ange hur lagstiftningen skulle kunna ändras på vissa områden. De lagstiftningsmässiga konsekvenserna av utredningens förslag har inte blivit ordentligt penetrerade. Dels kan det finnas behov av författningsändringar även på andra områden än de av utredningen angivna. Dels bygger de av utredningen skissade författningsändringarna inte på någon reell analys av hur de lagda materiella förslagen bäst kan implementeras genom lagstiftning.

När det gäller tillsynsfrågorna anser jag att utredningsmaterialet är alltför magert för att över huvud taget kunna ligga till grund för några förslag. Tillsynsproblematiken är synnerligen komplex och utredningen har inte gjort några egentliga överväganden. Dessutom utreds dessa frågor i annan ordning. Enligt min mening borde utredningen därför ha avstått från förslag i denna del.

Utredningen slår fast vissa principer för militär medverkan i civil verksamhet. Även denna fråga utreds i annan ordning och det kan inte uteslutas att den utredningen kan komma fram till andra ställningstaganden.