Säker information

Förslag till informationssäkerhetspolitik

Delbetänkande av InfoSäkutredningen

Stockholm 2005

STATENS OFFENTLIGA UTREDNINGAR

SOU 2005:42

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Tryckt av XGS Grafisk Service
Stockholm 2005

ISBN 91-38-22356-2
ISSN 0375-250X

Till statsrådet och chefen för Försvarsdepartementet

Genom beslut den 11 juli 2002 (dir. 2002:103) bemyndigade regeringen chefen för Försvarsdepartementet att tillkalla en särskild utredare med uppdrag att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten. Med stöd av regeringens bemyndigande kallade chefen för Försvarsdepartementet f.d. riksdagsledamoten Anders Svärd till särskild utredare (regeringsbeslut 2002:1743/CIV, protokoll Fö 2002:1744/EPS).

Utredningen antog namnet InfoSäkutredningen.

En delrapport om signalskydd lämnades till regeringen den 28 februari 2003 (SOU 2003:27).

Utredningens uppdrag utökades genom tilläggsdirektiv beslutat den 20 februari 2003 (dir. 2003:29). Den särskilde utredaren fick utöver det ursprungliga uppdraget i uppgift att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas, hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden samt hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras i Sverige. Utredaren fick dessutom i uppdrag att följa myndigheternas uppbyggnad av de verksamheter som regeringen aviserade i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158), angående informationssäkerheten i samhället.

Delrapporten Informationssäkerhet i Sverige och internationellt – en översikt, lämnades till regeringen den 1 april 2004 (SOU 2004:32).

Enligt tilläggsdirektiv beslutat den 7 april 2004 (dir. 2004:46) skall utredningen genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) vad avser de bedömningar när det gäller uppgiftsfördelningen som regeringen gjorde inom informationssäkerhetsområdet.

Kansliråd Ulf Johansson och departementssekreterare Julia Mikaelsson, ämnessakkunnig Richard Oehme och kansliråd Fredrik Sand har varit sakkunniga. Experter har varit avdelningschef John Daniels, överstelöjtnant Håkan Gustafsson, avdelningschef Anders Johanson, säkerhetschef Bo Karlsson, enhetschef Staffan Karlsson, chefsjurist Elisabeth Lager, överingenjör Mats Ohlin, avdelningsdirektör Kristina Starkerud (entledigad den 11 november 2004), avdelningsdirektör Anna-Karin Waldton och avdelningsdirektör Wiggo Öberg.

Kriminalinspektör Patrik Håkansson och IT-strateg Anders Nordh utsågs till experter i utredningen från och med den 1 juli 2004. Avdelningsdirektör Anna Larsson utsågs till expert den 11 november 2004 och Nils-Gunnar Forsberg adjungerades till utredningen den 10 december 2004.

Avdelningsdirektör Arne Jonsson och doktorand Anna Palbom entledigades som experter den 1 juli 2004. Anja Stegen entledigades den 13 december 2004 som sekreterare.

I det fortsatta arbetet har departementsråd Michael Mohr fungerat som huvudsekreterare och analytiker Josefin Grennert som sekreterare.

Konsult Bo Riddarström på BRi Konsult AB, har även i det fortsatta arbetet fungerat som en resursperson för utredningen.

Åke Pettersson, f.d. statssekreterare, har varit anlitad av utredningen, bland annat för frågor rörande kompetensförsörjning. Inom ramen för uppdraget genomfördes två scenarioövningar med utredningens sakkunniga, experter och myndighetsrepresentanter respektive med företrädare för näringslivet. Syftet med övningarna var att belysa ett antal centrala frågor närmare.

Genom tilläggsdirektiv beslutat den 28 april 2005 (dir. 2005:53), förlängs utredningens arbete. De organisatoriska aspekterna av utredningens förslag skall lämnas till regeringen den 9 september 2005. I sitt slutbetänkande återkommer utredningen till eventuella ekonomiska konsekvenser av de förslag som läggs.

Arbetssätt och förankring

Utredningen har fört en nära dialog med myndighetsrepresentanter, Sveriges Kommuner och Landsting samt företrädare för näringslivet, i syfte att fördjupa och förankra utredningens resonemang.

Frågor som rör hur näringslivet är konstituerat och organiserat är av betydelse för möjligheten att få en bred representation av

privat sektor, till exempel för samverkan med offentlig sektor, och viktigt underlag i utredningens arbete med att formulera en nationell strategi för informationssäkerhet. Med anledning av detta uppdrog utredningen åt Hans Holst att formulera en beskrivning av relevanta branscher med avseende på marknaden kring informationssäkerhet, vilka företag som ingår, storleken på dessa och andra faktorer som kan vara av betydelse.

Ett centralt begrepp i utredningens arbete är samhällsviktig verksamhet. Utredningen uppdrog åt Totalförsvarets forskningsinstitut (FOI) att utarbeta kriterier för bedömning av om en verksamhet är samhällsviktig.

Krisberedskapsmyndigheten (KBM) fick i uppdrag av utredningen att göra en beskrivning av hur informationssäkerhetsfrågor har organiserats i andra länder. Då utredningen kommer att föreslå organisatoriska förändringar först i sitt slutbetänkande i september 2005, behandlas inte dessa frågor i föreliggande betänkande.

Utredningen har sedan delbetänkandet den 1 april 2004 företagit studieresor till Australien och USA.

Avgränsning och ambition med delbetänkande tre

Utredningens ambition med det andra delbetänkandet var att presentera en bland relevanta aktörer förankrad bild av informationssäkerhetsarbetet i Sverige i dag. Bilden omfattade såväl påbörjat och planerat arbete, som gällande förutsättningar och begrepp inom området. Denna bild har använts som avstamp för utredningens vidare arbete med delbetänkande tre. Genom lägesbedömningen har olika aktörers arbete med informationssäkerhet och deras behov på området kunnat identifieras, vilket har varit en nödvändighet för utredningens formulerande av en välgrundad och genomförbar strategi för utvecklingen av informationssäkerhetsarbetet.

Föreliggande betänkande utgör utredningens förslag till principer för utveckling av informationssäkerheten. Förslagen baseras på identifierade behov på området, till exempel av författningsstöd, kompetensutveckling och samordning.

Utredningen överlämnar härmed delbetänkandet *Säker information. Förslag till informationssäkerhetspolitik* (SOU 2005:42).

Stockholm i maj 2005

Anders Svärd

/Michael Mohr
Josefin Grennert Johansson

Innehåll

Sammanfattning

Tillgång till korrekt och säker information vid rätt tillfälle är en förutsättning för tillväxt, konkurrens, utveckling, välfärd och trygghet i samhället. Det gäller alla – medborgare, företag och offentlig verksamhet.

Informations- och kommunikationstekniken har möjliggjort en explosionsartad utveckling inom informationsförsörjningen. Sverige innehar en framstående ställning internationellt i fråga om användning av ny teknik och redan genomförda investeringar i människor. Kompetens och teknik utgör en stor potential för framtiden.

Med ny teknik – där uppgifter och information bearbetas, lagras och förmedlas elektroniskt – följer inte bara ökade möjligheter, utan också problem i form av nya sårbarheter och beroenden. IT-utvecklingen har visat sig vara snabbare än förmågan att utveckla adekvat säkerhetstänkande.

Frågor kring sårbarheten berör ett mycket stort antal aktörer och intressen, och området präglas av stor dynamik. Det är svårare att värna säkerheten i moderna informations- och kommunikationssystem, där informationen lagras, bearbetas och förmedlas elektroniskt än när informationen föreligger i fysisk form. Detta ger även upphov till juridiska problem.

Bilden av dagens brister och hot är mycket komplex och därmed även behovsbilden. Därför behövs, enligt utredningen, en sammanhållen politik inom informationssäkerhetsområdet.

Det är nödvändigt att etablera vissa principer som kan ligga till grund för beslut om ansvarsfördelning och åtgärder i samhället. Två principer har utkristalliserats: den första handlar om hotets ursprung och den andra om hotets möjliga konsekvenser.

Enligt utredningens mening innebär den första principen att ansvaret för hanteringen av administrativa och tekniska säkerhetsbrister faller på den som är ansvarig för verksamheten. Detta följer även av ansvarsprincipen. Det utesluter dock inte att staten har ett

ansvar, t.ex. för vissa förebyggande åtgärder inom det privata området. Det kan vara svårt för enskilda och företag att skydda sig mot aktörsberoende, antagonistiska hot. Dessa hot kan mycket snabbt komma att kräva statliga insatser, särskilt när det gäller samhällsviktig verksamhet. Var gränsen mellan det privata och det offentliga åtagandet går är mycket svårt att slå fast.

Den andra principen innebär att ju svårare konsekvenser ett hot eller en brist kan leda till, desto mer sannolikt är det att staten kommer att involveras i någon form. I det statliga åtagandet bör därför ingå frågor om t.ex. krishantering, brottsbekämpning eller totalförsvar.

Med dessa starkt förenklade principer för arbets- och ansvarsfördelning inom informationssäkerhetsområdet som utgångspunkt kan fyra uppgifter eller handlingslinjer urskiljas: att förebygga, förbereda, förhindra respektive att hantera allvarliga störningar. Dessa är uppgifter som flertalet aktörer måste axla i en eller annan form. Två av dessa mål eller uppgifter ingår redan i regeringens strategi; förhindra och hantera.

Det finns ingen definitiv lösning på problemet med informationssäkerhet. Därtill är problemet alldeles för komplext och området dessutom under ständig utveckling. Utredningen anser dock att en gemensam, nationell strategi och en samverkansprocess skulle kunna lära oss att leva med problem som rör informationssäkerhet. En av utredningens huvuduppgifter är därför att se utvecklingsmöjligheter i den av regeringen angivna strategin för informationssäkerhet.

Övergripande målsättning för informationssäkerheten

Regeringens övergripande målsättning är att upprätthålla en hög informationssäkerhet i hela samhället, som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet.

Strategin för att nå detta mål, liksom för övrig krishantering i samhället, måste utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. Utredningen delar regeringens bedömning.

Ett dilemma för utredningen

I utredarens uppdrag ingår att utarbeta förslag till hur den svenska informationssäkerheten kan förbättras och överväga vad den enskilda medborgaren kan göra, vad som bör falla på enskilda företag och vad som kan lämnas till marknaden respektive vad som faller inom det offentliga åtagandet. Utredningen har också sett som sin uppgift att överväga vilka administrativa respektive tekniska åtgärder som kan aktualiseras, liksom vilka olika former av administrativa, ekonomiska och informativa styrmedel som bör användas i sammanhanget.

Utredningen beklagar att detta delbetänkande har kommit att domineras av överväganden som rör det offentliga agerandet – särskilt det statliga – och de tekniska aspekterna av informationssäkerhet. Detta är en konsekvens av utredningens direktiv, som i flera fall är direkta beställningar som rör statens eget agerande och som därför nödvändiggör en fördjupning av resonemangen. Detta bör inte uppfattas som ett uttryck för var utredningen anser att tyngdpunkten i informationssäkerhetsarbetet bör ligga.

En nationell strategi

Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) i grunden är riktig. Utredningen har dock funnit anledning att konkretisera och fördjupa den. I regeringens strategi ingår även vissa organisatoriska åtgärder. Utredningen har tagit fram underlag för utvärdering och återkommer till dessa frågor i slutbetänkandet.

Utredningen framhåller att en strategi för informationssäkerhet måste kunna inrymma många aspekter, tidsperspektiv, mål och medel eftersom den syftar till att sammanfatta en handlingslinje på lång sikt. Strategin skall kunna ligga till grund både för privata och offentliga aktörer. En ökad informationssäkerhet måste därför bygga på att regeringen i en nationell strategi lyckas fånga in frågeställningar som kan omfattas av flertalet aktörer och intressenter.

Mot bakgrund av de resonemang som redovisas i kapitel 3 och 4 föreslår utredningen en strategi som innefattar att:

1. utveckla Sveriges position inom EU och i internationella sammanhang
2. skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet
3. främja ökad användning av IT
4. förebygga och kunna hantera störningar i informations- och kommunikationssystem
5. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen
6. förstärka förmågan inom området nationell säkerhet

I strategin bör även ingå att:

7. utnyttja samhällets samlade kapacitet
8. fokusera på samhällsviktig verksamhet
9. öka medvetenheten om säkerhetsrisker och möjligheter till skydd
10. säkerställa kompetensförsörjningen

Den internationella dimensionen

Utredningen har valt att inledningsvis betona att de europeiska och de internationella sammanhangen är av strategisk betydelse. Informationssäkerhet är ett gemensamt, internationellt problem och de strategiska lösningarna måste därför utvecklas i samverkan med andra länder – både inom EU och i internationella organ. En bred tillämpning av OECD:s riktlinjer är därvid ett viktigt steg. Förmågan att samordna arbetet behöver utvecklas, dels för att fullfölja svenska positioner och åtaganden, men också för att bättre ta tillvara de erfarenheter som andra internationella aktörer gör.

Att skapa förtroende och främja ökad användning av IT

Den andra punkten är liksom den tredje punkten nationell till sin karaktär i den meningen att ansvar, befogenheter och resurser redan finns. Utredningen vill betona att den ökade informationssäkerheten skall stödja en svensk utveckling av näringsliv och offentlig sektor och skall främja en demokratisk utveckling och ökad trygghet för medborgarna. Detta innebär att förtroendet för informationsförsörjning måste kunna upprätthållas, även när den sker elektroniskt. En

väl fungerande informationsförsörjning bygger på att informationssäkerheten kan utvecklas, vilket i sin tur är en förutsättning för ökad användning av IT. Detta är också en förutsättning för tillväxt, konkurrens och utveckling.

Att förebygga, förbereda, förhindra, upptäcka, hantera och ingripa vid störningar

I regeringens övergripande strategi ingår formuleringen att ”kunna förhindra och hantera störningar i samhällsviktig verksamhet”. Utredningen menar att strategin bör tydliggöra vikten av förebyggande och förberedande åtgärder. Vidare betonar utredningen att begreppet hantera måste inkludera förmågan att i olika former upptäcka, ingripa och agera i samband med störningar – till exempel genom brottsbekämpning.

Dessa kompletteringar skall klargöra att informationssäkerhetsarbete måste omfatta alla skeden och flera aktörer. Det innebär att den förebyggande uppgiften och de förberedande åtgärderna måste bli en del av många myndigheters sektorsansvar och instruktionsmässiga uppgift. Utredningen föreslår vidare att regeringens strategi i denna fråga preciseras till att avse störningar i informations- och kommunikationssystem. Frågan om prioriteringar av samhällsviktig verksamhet bör behandlas som en särskild punkt i strategin.

Att förstärka underrättelse- och säkerhetstjänsterna och att förbättra delgivningen

Regeringen har tidigare konstaterat att underrättelse- och säkerhetstjänsternas arbete bör förstärkas för att förhindra allvarliga informationsattacker mot svenska intressen. Utredningen delar denna uppfattning, men framhåller samtidigt att flera aktörer måste kunna få del av underrättelseinformation för att kunna beakta denna i sitt eget säkerhetsarbete. Utredningen är väl medveten om de restriktioner och svårigheter som ligger i uppgiften men framhåller ändå att bearbetning och delgivning av underrättelseinformation måste utvecklas i syfte att ge underlag för alla aktörer med uppgifter inom informationssäkerhetsområdet.

Att förstärka förmågan inom området nationell säkerhet

I det statliga åtagandet ingår frågor om nationell säkerhet i vid mening – till exempel krishantering, brottsbekämpning, kontraterrorism eller totalförsvar. För att möta de mest kvalificerade hoten krävs, enligt utredningens mening, en förstärkt förmåga att upptäcka och analysera störningar liksom en förmåga att kunna ingripa och agera kraftfullt mot antagonistiska och/eller kriminella aktörer. Utan en helhetssyn på de tekniskt relaterade hoten kan staten inte skydda samhället från kvalificerade aktörers angrepp på svenska informationssystem. En sådan helhetssyn förutsätter tillgång till relevant information, kompetens och teknisk utrustning. Detta är frågor som kräver långsiktighet och uthållighet och därför bör innefattas i en nationell strategi.

I de första sex punkterna har utredningen försökt sammanföra frågeställningar och överväganden som handlar om strategiska målsättningar. Utredningen har även funnit anledning att föreslå inriktning och prioriteringar av det framtida informationssäkerhetsarbetet.

Att utnyttja samhällets samlade kapacitet

Utredningen föreslår att utgångspunkten för informationssäkerhetsarbetet bör vara att bättre utnyttja samhällets samlade kapacitet på området. De investeringar som redan gjorts i människor, kompetens och teknik utgör en värdefull potential för framtiden. Ökad informationssäkerhet handlar därför, enligt utredningens synsätt, inte i första hand om ytterligare investeringar utan snarare om en tydligare ansvars- och arbetsfördelning mellan samhällets olika aktörer. Den tekniska utvecklingen på IT-området är i allt väsentligt styrd av olika privata aktörer på marknaden. Eftersom utvecklingen sker på marknaden är det också i första hand där som säkerhetslösningar måste utvecklas. Inom samhällsviktiga områden måste därför aktörerna inom offentlig sektor utveckla sina förutsättningar och sin förmåga som kravställare och beställare.

Samverkan privat – offentligt

Enligt utredningens mening borde det vara möjligt att inom ytterligare sektorer/områden utveckla samverkan i syfte att öka informationssäkerheten. Utredningen har vid flera tillfällen kunnat konsta-

tera att näringslivet välkomnar en bredare samverkan kring informationssäkerhet till ömsesidig nytta, men att denna samverkan måste vara frivillig. Staten måste därför hitta former för en dialog med näringslivet som får anpassas till varierande förutsättningar. Det staten kan göra handlar då om att tydliggöra sin egen uppgift och att peka ut en myndighet med sammanhållande ansvar. Att utveckla former för samverkan mellan det privata och offentliga är av strategisk betydelse.

Samverkan inom offentlig sektor

Utredningen har konstaterat att staten i stort sett har samma problem att hantera som Sveriges kommuner och landsting. Förutsättningarna för samverkan inom staten respektive mellan kommunerna företer också många likheter. Det kan enligt utredningen finnas skäl att genom en särskild överenskommelse bekräfta en samsyn i informationssäkerhetsfrågor och att tydliggöra att kommuner och landsting kan disponera tillgängliga statliga medel även för dessa ändamål.

Det privata åtagandet

Varje enskild verksamhetsansvarig ansvarar själv för leveranssäkerheten och kvaliteten i sin verksamhet. Informationssäkerhet – såväl teknisk som administrativ – måste ses som en integrerad del av verksamhetsansvaret och skiljer sig på så vis inte nämnvärt från andra typer av säkerhetsfrågor. Åtagandet skulle således följa ansvarsprincipen.

Enligt utredningens mening måste det ligga inom varje medborgares eget ansvar att inhämta kunskaper och vara medveten om de säkerhetsrisker som följer med elektronisk hantering. På motsvarande sätt anser utredningen att det i princip måste ligga inom varje företags åtagande att svara för såväl kompetensförsörjning som säkerhet i de egna informationssystemen. I det privata åtagandet måste även ingå att säkerställa säkerheten i de fall någon utomstående anlitas för tjänster av olika slag.

För samhällsviktig verksamhet och system finns det dock anledning för staten att ställa särskilda krav på leveranssäkerhet och kvalitet, vare sig verksamheten drivs av privat eller enskild. Ett problem som utredningen lyfter fram är att det hittills inte har funnits

några kriterier för vad som skulle kunna betraktas som samhällsviktig verksamhet.

Det offentliga åtagandet

Det grundläggande synsätt som utredningen redovisat på det privata åtagandet är till största del tillämpligt även på verksamheten hos myndigheter och organ inom offentlig sektor. All verksamhet skulle således innefatta ett samlat ansvar för kompetensförsörjning och säkerhet i de egna informations- och kommunikationssystemen.

Det statliga åtagandet

Enligt utredningens mening är det av stor vikt för samtliga aktörer att statens åtagande preciseras. Även om statens möjligheter att styra andra aktörer är begränsad så tydliggörs i vart fall indirekt vad staten anser bör ingå i andra aktörers ansvar. Statens åtagande, ansvar och intresse har därför av utredningen sammanfattats i följande fyra punkter:

1. Staten har ett övergripande ansvar för att en helhetssyn etableras och appliceras på informationssäkerheten och att nationella intressen bevakas inom EU och i internationella sammanhang.
2. Staten har ansvaret för samhällets spelregler inom informationssäkerhetsområdet.
3. Staten har ett särskilt ansvar för informationssäkerheten inom ett antal politikområden. Det gäller statens kärnverksamhet som till exempel rättsväsendet och underrättelse- och säkerhetstjänsterna. Det gäller även ansvaret för att olika samhällsviktiga verksamheter (el, tele etc.) bedrivs med tillräcklig säkerhet oavsett vem som äger dem.
4. Staten har slutligen ett eget intresse och ansvar för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sina olika roller som ansvarig för myndighetsutövning, i sin ägarroll etc.

Att fokusera på samhällsviktig verksamhet

Utredningen menar, liksom regeringen, att det av flera skäl är nödvändigt att fokusera ansträngningarna till sådana verksamheter som är av vital betydelse för samhällets funktioner. En verksamhet måste således betraktas som samhällsviktig om ett bortfall eller en störning av denna skulle få allvarliga konsekvenser för en eller flera samhällsfunktioner. Det är uppenbart att leveranssäkerheten och kvaliteten i den tekniska infrastrukturen kommer att vara beroende av hur informationssäkerheten i dessa system utvecklas. Men även många andra samhällstjänster är beroende av säkerheten i informations- och kommunikationssystemen. En helhetssyn på informationssäkerheten i samhällsviktiga verksamheter blir därför allt viktigare. Eftersom samhällets resurser inte är obegränsade kommer därför en prioritering mellan samhällsviktiga verksamheter också att vara av strategisk betydelse.

I dag finns inga av regeringen fastlagda kriterier eller definitioner som kan ligga till grund för urvalet. Utredningen föreslår därför att regeringen, med stöd av det underlag som har framtagits under utredningens arbete, konkretiserar vilka verksamheter som är samhällsviktiga och därmed kan bli föremål för särskilda åtgärder.

Att öka säkerhetsmedvetandet

IT-området utvecklas snabbare är säkerhetsmedvetandet. Det ökade IT-användandet har lett till ett ökat beroende av säkerhet och kvalitet i olika tjänster men medvetandet om sårbarheter, hot och risker är i dagsläget mycket lågt hos enskilda användare. Detsamma gäller kunskapen om vilka skyddsåtgärder som finns och erbjuds på marknaden. Enligt utredningens mening är medvetandet i dag så dåligt och bristerna så utbredda att särskilda insatser är motiverade under lång tid.

Att säkerställa kompetensförsörjningen

Enligt utredningens mening är det av strategisk betydelse att kunna säkerställa kompetensförsörjningen inom informationssäkerhetsområdet. Utredningen konstaterar också att staten behöver egen och unik kompetens. Dels har staten krav på sig att ta ansvar för samhället oavsett konjunkturer eller annat som styr efterfrågan på

kompetens. Staten har också det yttersta ansvaret för den nationella säkerheten, vilket ställer särskilda krav. Utredningen konstaterar att Sverige inte har tillräckliga resurser för att bygga dubbla strukturer. Därför krävs informationsutbyte och samarbete mellan den offentliga sektorn och näringslivet. Överväganden och förslag redovisas närmare i kapitel 8 om kompetensfrågor.

Strategi – samverkan – regelverk

I ovanstående tio punkter har utredningen sammanfattat sin syn på vad som bör ingå i en nationell informationssäkerhetsstrategi. Strategin har ett långsiktigt perspektiv och skall kunna ligga till grund för handlingsplaner, prioriteringar och åtgärder på två till tre års sikt, vilka kan förnyas utifrån ändrade omständigheter. Strategin vänder sig till alla aktörer – såväl privata som offentliga. Strategin kan ligga till grund för att öka informationssäkerheten i samhället genom en kontinuerlig process. Strategin förutsätter därför att formerna för samverkan utvecklas. Dessutom krävs ett modernt regelverk som stödjer, framtvingar eller tydliggör krav på aktörerna och som säkerställer att säkerheten efterlevs.

Styrmedel

Staten förfogar över en rad administrativa, ekonomiska och informativa styrmedel. I praktiken är dessa relativt svagt utvecklade på informationssäkerhetsområdet och utredningen lämnar därför förslag till inriktning av fortsatt författningsarbete och tillämpning av standard. Utredningen menar att en målstruktur för informationssäkerhet skulle kunna medverka till en sammanhållen politik på området.

Regeringen anmälde i propositionen prop. 2001/02:158 Samhällets säkerhet och beredskap att man hade för avsikt att göra en översyn av de rättsliga aspekterna, inklusive de internationella, på området informationssäkerhet. Utredningen kan konstatera att någon samlad översyn ännu inte har påbörjats, även om vissa författningsändringar har genomförts på enstaka delområden. Detta har verkat återhållande på möjligheterna till ett samlat grepp i utredningen. Med tanke på den stora betydelse som informationssäkerheten har för all samhällsviktig verksamhet föreslår utredningen, i avvaktan på en

översyn av hela området, att regeringen prövar möjligheten att genom författningar lägga grunden för vissa åtgärder inom området. Behovet av en tillfredställande informationssäkerhet är inte begränsat till verksamheter som är av betydelse för rikets säkerhet eller skyddet mot terrorism. Behovet är inte heller begränsat till information som är hemlig enligt sekretesslagen (1980:100) eller som är känslig ur ett integritetsperspektiv osv. Behovet av säkerhet för information kan – som utredningen tidigare har pekat på – göra sig lika starkt gällande även på andra områden. Utredningen har därför förordat en bred definition av begreppet informationssäkerhet, med utgångspunkt i EU:s säkerhetsbestämmelser. Enligt dessa syftar informationssäkerheten till att främja tillväxt, konkurrens och välfärd. För uppgifter som lagras, bearbetas och överförs i elektronisk form skall säkerheten uppfyllas genom krav på konfidentialitet, okränkbarhet och tillgänglighet.

Bestämmelser om informationssäkerhet finns i flera olika författningar. Det saknas dock ett heltäckande och sammanhållet regelverk på informationssäkerhetsområdet som motsvarar utredningens bredare definition av begreppet informationssäkerhet. Enligt utredningen finns det därför ett behov av ett utvidgat regelverk.

Utredningen visar möjliga vägar att gå för att åstadkomma ett sådant regelverk. En väg skulle vara att utöka tillämpningsområdet för nuvarande säkerhetsskyddslagstiftning. En annan väg skulle vara en helt ny lag på informationssäkerhetsområdet. Framtagandet av ett sådant regelverk, som utredningen anser att det finns ett stort behov av, måste dock föregås av en mycket mer omfattande och djupare analys än vad denna utredning har möjlighet att göra. Frågan om ett mera sammanhållet och heltäckande regelverk på informationssäkerhetsområdet måste därför utredas i särskild ordning.

Utredningen anser dock att den har stöd för att redan nu föreslå lagstiftningsåtgärder för att råda bot på brister i dagens regelverk. Utredningen föreslår en ny förordning om vissa åtgärder för informationssäkerhet hos staten. Genom detta förslag kan staten ta initiativ och driva på det praktiska säkerhetsarbetet hos myndigheterna. Detta kan i sin tur utgöra riktvärde för andra aktörers arbete. Vidare föreslår utredningen att begreppet informationssäkerhet utmönstras ur säkerhetsskyddslagstiftningen, och ersätts med begreppet sekretessäkerhet.

Enligt utredningen finns starka motiv för att stärka säkerheten i nätsäkerhetsrelaterade frågor. Riksdagens Trafikutskott har också

tagit vissa initiativ i dessa frågor och från den 1 juli 2005 gäller utvidgade tillämpningsbestämmelser för säkerheten. Enligt utredningens mening handlar det därutöver om att förstärka möjligheterna att ställa tydligare krav på leveranssäkerhet och kvalitet. Andra aspekter av säkerheten handlar om filtreringsfrågor samt hantering av vissa abonnentuppgifter. Utredningen stödjer Post- och telestyrelsens (PTS) ambitioner i denna fråga.

Standardiseringen på informationssäkerhetsområdet har i dag kommit långt. Informationssäkerhet är ytterst en fråga om kvalitetstänkande. När det gäller hantering och utbyte av elektronisk information är det av vikt att det bygger på standarder. Fördelarna är många. Utredningens uppfattning är att staten bör verka för en bred användning av standarder inom statlig verksamhet.

Försvarets materielverk (FMV) har sedan tidigare ett uppdrag att bygga upp en svensk certifieringsordning för Common Criteria. Mot bakgrund av erfarenheter från andra länder är det troligt att Försvarsmakten och andra myndigheter med mycket höga sekretesskrav kommer att vara de viktigaste intressenterna för certifierade produkter och program. Tillgång till certifierade produkter underlättar samtidigt för alla myndigheter, företag och andra som önskar upphandla produkter med hög säkerhet.

Ledningssystem för Informationssäkerhet (LIS) är en anvisning för hur man åstadkommer ett ledningssystem. Standarden är inte ett ledningssystem i sig. LIS omfattar hela informationssäkerhetsbegreppet och fokuserar på de risker och hot som kan uppkomma inom en organisation. Tillämpning leder till förbättrade administrativa och tekniska rutiner. LIS används med framgång inom flera större svenska företag. Staten bör använda LIS inom den offentliga verksamheten.

Den verksamhetsstruktur som finns inom svensk statsförvaltning innebär i regel att mål formuleras på flera nivåer. Strukturen syftar till att tydliggöra hur verksamheter på skilda nivåer bidrar till att uppfylla målen inom ett politikområde. Som en följd av detta skiljer målen sig i precision mellan nivåerna.

Informationssäkerhet kan formuleras som ett verksamhetsområde eller en del av ett politikområde. Det berör många politikområden och flera utgiftsområden. Informationssäkerhet kan ses som en förutsättning för övriga verksamheter. Utredningen förordar i första hand att informationssäkerhet ses som ett verksamhetsområde.

Redan detta innebär ett visst ställningstagande i finansieringsfrågan. Med utgångspunkt i ansvarsprincipen är det rimligt att finansiering

av informationssäkerhet i huvudsak sker genom ordinarie anslag för verksamhetsområdet till respektive myndighet. Detta bör enligt utredningen vara huvudprincipen för finansieringen och den finansiella styrningen av informationssäkerhet. Det är dock enligt utredningen motiverat att även i framtiden – särskilt för ändamål som kan ses som långsiktiga investeringar i en högre informationssäkerhet – behålla möjligheterna till kompletterande finansiering av informationssäkerhet via den så kallade civila ramen. Utredningen avser att återkomma till dessa frågor i sitt slutbetänkande.

Kompetensfrågor

Säkerhetsmedvetandet har under de senaste åren höjts i näringsliv och myndigheter liksom hos enskilda IT-användare. En rad åtgärder måste dock vidtas för att ytterligare förbättra säkerhetsmedvetandet och öka kunskaperna om informationssäkerhet. Det bör ske bland annat inom ramen för utbildningssystemet. Lärarutbildningen måste förbättras. Blivande lärare erhåller för lite utbildning vad gäller IT-användning och -teknologi.

I såväl grund- som gymnasieskolan bör ett säkerhetsmedvetande, anpassat till respektive ålders behov och förutsättningar, byggas in i den grundläggande data- och IT-utbildningen.

En betydande del av utbildningsbehovet måste tillgodoses inom högskolans ram. Kopplingen mellan utbildning och forskning måste stärkas. Informationssäkerhet bör utgöra en baskunskap för många yrkesgrupper, t.ex. jurister, samhällsvetare, lärare, ekonomer och tekniker.

På senare år har allt fler företag inrättat funktionen informationssäkerhetschef. Motsvarande behov av sådana befattningar finns inom myndighetsvärlden. Utredningen anser att det finns skäl att stimulera till etablering av kvalificerad utbildning i informationssäkerhet på magisternivå för att bland annat tillgodose efterfrågan av tjänster inom området.

Forskning

De växande behoven av säkra informationssystem ställer krav på ökade resurser för forskning inom informationssäkerhet. Krisberedskapsmyndigheten (KBM) har ett särskilt ansvar inom forsk-

ningsområdet för att stimulera, initiera och delvis även finansiera forskning inom området informationssäkerhet. Det gäller både för forskning inom det allmänna universitets- och högskoleområdet och inom ramen för Försvarshögskolans (FHS) och Totalförsvarets forskningsinstituts (FOI) verksamhet. Detta ansvar behöver förtydligas ytterligare.

Att säkra rikets ledning av och tillgång till samhällsviktig infrastruktur ställer stora krav på säkerhet i informationshanteringen. Staten måste därför vara bidragande till att det byggs upp en forskarkompetens inom området informationssäkerhet. Forskningsbaserad kunskap bygger på långsiktighet och uthållighet i projektsatsningar och i kompetensutveckling bland berörda forskare.

Krisberedskapsmyndigheten (KBM) bör därför utveckla ett tematiskt område kring informationssäkerhet. Forskargrupper som erhåller anslag skall veta att satsningen är flerårig.

Försvarshögskolans samarbete med internationella högskolor och universitet kan bidra till att utveckla utbildningen inom informationssäkerhet. En utbildning i informationssäkerhet skulle kunna ske med en praktisk inriktning för certifiering av nyckelpersonal inom myndigheter och företag.

Totalförsvarets forskningsinstitut (FOI) skall verka för samordning mellan militär och civil, respektive mellan nationell och internationell forskning. Vid avdelningen för försvarsanalys bedrivs studier och forskning inom området informationssäkerhet på olika systemnivåer. Under senare år har kunskapsutveckling skett vad gäller säkring av viktig infrastruktur, där bland annat frågor om informationssäkerhet får en allt mer framträdande roll.

Forskning inom informationssäkerhetsområdet bedrivs även inom andra organisationer. The Swedish Institute of Computer Science, Sics, ägs till tre fjärdedelar av svensk industri och en fjärdedel av staten och är således ett exempel på område där privat och offentlig samverkan har utvecklats. Målet är att bidra till konkurrensförmågan hos svensk industri genom att bedriva avancerad forskning inom strategiskt viktiga områden av datavetenskap samt att aktivt främja användningen av nya idéer och resultat i industrin och samhället i stort. Sics har inte primärt fokus på informationssäkerhet, men i praktiken berör en stor del av forskningen frågor om funktionalitet och säkerhet. Sics fyller tillsammans med övriga institut en mycket viktig funktion genom att vara en avancerad brygga mellan näringslivets forskningsbehov och statens behov av att främja forskningen och forskarvärlden inom IT-området. Enligt utredningens mening

är det angeläget att institutets forskning även i framtiden omfattar projekt inom informationssäkerhetsområdet.

Europeiska unionen

EU initierar och finansierar en omfattande forskning inom informationsteknikens område. Förberedelserna för det sjunde utvidgade ramforskningsprogrammet har nu påbörjats. Informationssamhällets teknik (IST) inom det sjätte ramforskningsprogrammet har haft en budget på 3.6 miljoner Euro under fyra år. Inom IST finns fyra huvudprioriteringar: för det första informationssamhällets teknik som berör samhälleliga och ekonomiska utmaningar, för det andra teknik för kommunikation, hantering av information och programvara, för det tredje komponenter och mikrosystem och för det fjärde teknik för kunskapshantering och intelligenta gränssnitt. Främst det första området berör informationssäkerhet. Antalet projekt är mycket stort.

Sverige bör ha en hög ambition att delta i EU:s policyskapande arbete för att inrikta forskningen inom informationssäkerhetsområdet och som genomförare av större forskningsprojekt inom området. Det är en angelägen uppgift både för Regeringskansliet och myndigheter som Krisberedskapsmyndigheten och Vinnova, liksom för svenskt näringsliv och högskole- och universitetsvärlden, att delta i arbetet och få del av de betydande forskningsresurser som EU kommer att satsa under kommande år inom informationssäkerhetsområdet. Det kräver också ett utvecklat samarbete med partners i andra EU-länder.

Kryptologisk kompetens

Kryptering har länge varit en avancerad disciplin, som kräver mycket hög kompetens. Till skillnad från tidigare krävs numera även hög IT-kompetens. Med IT-revolutionen har kryptering blivit en angelägenhet långt utanför det militära området.

Näringsliv och myndigheter måste ha hög kompetens i datasäkerhet. Däremot är det inte nödvändigt att alla har tillgång till egna kryptologer. Ur kompetenssynpunkt räcker det dock inte med några få personer i Sverige med hög kompetens inom kryptologi. För att stimulera tillväxten av särskild kompetens för samhället och

större företag kan exempelvis sponsring eller finansiering av doktorandtjänster vid universiteten komma i fråga.

Beställarkompetens och revision

Samhället har enligt utredningens bedömning låg beställarkompetens för informationssäkerhet. Detta utgör ett grundläggande problem. Staten har ett ansvar för att utveckla beställarkompetensen. Tillgång till certifierade produkter enligt Common Criteria eller tjänster enligt Ledningssystem för informationssäkerhet (LIS) skulle avsevärt underlätta upphandling av informationssäkerhet. Det krävs också en satsning på fortbildning i upphandlingsteknik inom området informationssäkerhet. Särskild uppmärksamhet bör ägnas kompetens i avtalsfrågor.

Revision av informationssäkerhet bör utvecklas i flera former, dels som en del av den årliga revisionen – särskilt vad avser redovisnings- och affärssystem, dels genom sårbarhets- och riskanalyser och tester av informationssäkerheten samt genom tillämpning av standarden Ledningssystem för informationssäkerhet (LIS).

Informationssäkerhet är en ledningsfråga. Behovet av fortbildning gäller även den verkställande nivån samt styrelsenivån i myndigheter och företag. Varje myndighet, företag, kommun, landsting eller annan organisation har ett eget ansvar för att se till att alla medarbetare som har uppgifter inom området informationssäkerhet erhåller adekvat fortbildning.

Signalspaning som skydd för IT-system

Signalspaning har betydelse för möjligheten att skydda samhällsviktiga system mot kvalificerade IT-relaterade hot. Utredningen vill peka på att det finns kvalificerade IT-relaterade hot som med den framväxande globala kommunikationsstrukturen och den nya IT-tekniken i förlängningen också kan innebära hot mot rikets säkerhet. Dessa hot utgör också hot mot många andra verksamheter. Gränsen mellan allmänna hot och hot mot rikets säkerhet är inte absolut.

Ett av de främsta medlen, förutom det förebyggande arbetet, för att möta kvalificerade IT-relaterade hot är att inrikta vår underrättelsetjänst mot dem. Detta understryks också i regeringens hit-

tillsvarande strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas och delgivningen av erfarenheter utvecklas. Dessa myndigheters möjligheter att spela en avgörande roll för skyddet mot kvalificerade IT-relaterade hot bedöms som stora.

Sverige har under lång tid haft en framträdande plats i Europa vad gäller kryptologisk kompetens och förmåga. Den, relativt sett, successivt försvagade beräkningskraften genom brist på resurser för inköp av ny snabb datorkraft riskerar dock att på sikt allvarligt försämra Sveriges samlade kompetens på området.

Signalspaning kan först och främst bidraga till underrättelser avseende hot och aktörer som agerar mot svenska informationssystem. En lika viktig del är att kunskap om brister i olika tekniska informationssystem erhålls i den egna underrättelseverksamheten genom signalspaning. Det ger också kunskaper för utveckling och certifiering av IT-program och produkter. Sådan kunskap bör kunna användas till skydd för samhällsviktiga system.

Fortsatt arbete

Utredningens redovisning och förslag i detta delbetänkande är avsett att kunna ligga till grund för fortsatt informationssäkerhetsarbete och för en sammanhållen politik på området. Flera av de överväganden och förslag som redovisas har även konsekvenser för hur staten fördelar sina resurser och organiserar den egna verksamheten. Utredningen återkommer till dessa frågor i sitt slutbetänkande i september 2005.

Författningsförslag

1. Förslag till förordning (0000:000) om vissa åtgärder för informationssäkerhet hos staten

Härigenom föreskrivs följande:

Inledande bestämmelser

1 § I denna förordning ges bestämmelser om vissa åtgärder för att säkerställa administrativ och teknisk informationssäkerhet hos statliga myndigheter under regeringen.

Bestämmelserna i denna förordning skall tillämpas bara om något annat inte följer av lag eller annan förordning.

2 § Med administrativ och teknisk informationssäkerhet avses i denna förordning säkerhet vid hantering av elektroniska system för bearbetning, lagring och överföring av information, för att i den elektroniska hanteringen säkerställa informationens konfidentialitet, okränkbarhet och tillgänglighet.

3 § En myndighet skall säkerställa den administrativa och tekniska informationssäkerheten genom att vidta de administrativa och tekniska åtgärder som anges i 4–8 §§.

Regeringen kan besluta att de myndigheter som anges i bilagan till denna förordning skall tillämpa särskilda säkerhetskrav utöver de grundkrav som anges i förordningen.

Administrativa åtgärder

Informationssäkerhetsplan

4 § Myndigheten skall upprätta riktlinjer för informationssäkerheten och en årlig plan för administrativa och tekniska åtgärder inom

myndigheten för att säkerställa att ställda krav på informationssäkerhet uppnås.

Planen skall utformas med hänsyn till övriga krav som ställs i verksamheten. Planen skall innehålla en redovisning av de systemspecifika säkerhetskrav som utarbetas av myndigheten för driften av IT-system. Redovisningen av systemspecifika säkerhetskrav skall vara fullständig och tydlig samt ange de säkerhetsprinciper som skall följas och vilka detaljerade säkerhetskrav som skall uppfyllas. Planen skall även innehålla en översikt över de åtgärder som genomförts enligt 5–8 §§.

Informationssäkerhetsansvarig

5 § Hos myndigheten skall det finnas en informationssäkerhetsansvarig som utövar kontroll över informationssäkerheten. Den informationssäkerhetsansvarige skall i dessa frågor vara direkt underställd myndighetens chef. Det skall finnas ersättare för den informationssäkerhetsansvarige.

Behörighet

6 § Tillgång till viss utrustning eller information som är specifik för systemens säkerhet skall kräva särskild behörighet.

Utbildning

7 § Myndigheten skall se till att personal med arbetsuppgifter där hantering av elektroniska system för bearbetning, lagring och överföring av information ingår får utbildning om informationssäkerhet.

Tekniska åtgärder

8 § Myndigheten svarar för att tekniska åtgärder vidtas så att sådan utrustning m.m. som används för, eller stödjer användandet av, system vid elektronisk bearbetning, lagring och överföring av information uppfyller grundläggande krav på informationssäkerhet. Myndigheten svarar även för att kraven på informationssäkerheten

kan upprätthållas då utomstående anlitas för tjänster som rör myndighetens informations- och kommunikationssystem.

För myndigheter som anges i bilagan till denna förordning kan enligt 3 § andra stycket därutöver gälla särskilda krav på tekniska åtgärder.

Tillsyn

9 § Informationssäkerheten enligt denna förordning skall kontrolleras av den myndighet som regeringen bestämmer.

10 § Om det vid tillsynen över informationssäkerheten enligt denna förordning framkommer brister som trots påpekande inte rättas till av den ansvariga myndigheten, skall tillsynsmyndigheten anmäla förhållandet till regeringen.

Verkställighetsföreskrifter

11 § Den myndighet som regeringen bestämmer skall meddela närmare föreskrifter om de administrativa och tekniska åtgärder som skall vidtas för att uppfylla grundläggande och särskilda krav på informationssäkerhet vid hantering av elektroniska system för bearbetning, lagring och överföring av information.

Denna förordning träder i kraft den …

2. Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 7 och 9 §§ säkerhetsskyddslagen (1996:627) skall ha följande lydelse.

7 § Säkerhetsskyddet skall förebygga

1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (sekretessäkerhet),

2. att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning), och

3. att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet *(säkerhetsprövning)*.

Säkerhetsskyddet skall även i övrigt förebygga terrorism.

Sekretessäkerhet

9 § Vid utformningen av *sekretessäkerheten* skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt.

Denna lag träder i kraft den ...

3. Förslag till förordning om ändring i säkerhetsskyddsförordningen (1996:633)

Härigenom föreskrivs att 9 och 13 §§ säkerhetsskyddsförordningen (1996:633) skall ha följande lydelse:

Sekretessäkerhet

9 § Hemliga handlingar som är av synnerlig betydelse för rikets säkerhet skall inventeras minst en gång per år.

Andra hemliga handlingar skall inventeras i den omfattning som anges i föreskrifter enligt 45 §.

13 § Myndigheter och andra som förordningen gäller för skall, innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, förvissa sig om att det för uppgifterna där finns fullgod *sekretessäkerhet*.

Denna förordning träder i kraft den ...

1 Utgångspunkter för utredningen

1.1 Regeringens strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system

Enligt den bedömning regeringen gjorde i proposition 2001/02:158 Samhällets säkerhet och beredskap bör den övergripande målsättningen vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna *förhindra* eller *hantera* störningar i samhällsviktig verksamhet.

I propositionen anfördes att strategin för att uppnå detta mål, liksom övrig krishantering i samhället, bör utgå från *ansvarsprincipen, likhetsprincipen* och *närhetsprincipen*, det vill säga att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande.

En viktig roll för staten anfördes därför vara att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilde systemägaren.

Vidare borde underrättelse- och säkerhetstjänstens arbete förstärkas för att förhindra allvarliga informationsattacker mot Sverige.

Sammanfattningsvis anfördes i propositionen att strategin för informationssäkerhet

- bör vara långsiktig
- bygga på ansvarsprincipen
- staten bör komplettera med åtgärder inom vissa särskilda områden
- utgör ingen statisk lösning, syftet är att bygga upp kompetens och resurser
- kräver lagstiftningsåtgärder som behöver genomföras
- kräver organisatoriska åtgärder

Beroendet av informationssystem leder till att behovet av kompetens ökar liksom behov av kvalificerat stöd.

Regeringen ansåg mot denna bakgrund att det är angeläget att samhällsviktiga system har en hög säkerhetsnivå och att insatserna för informationssäkerheten ökas. Angrepp via informationssystem riktade mot samhället (så kallade informationsoperationer) skall förhindras och Sveriges intressen inom det internationella informationssäkerhetsarbetet skall främjas.

Regeringen aviserade sin avsikt att inrätta fyra funktioner i syfte att förbättra informationssäkerheten. Dessa var omvärldsanalys, IT-incidenthantering, teknikkompetens, samt ett system för evaluering och certifiering. Avsikten var att uppgifterna skulle läggas på de myndigheter som redan hade näraliggande uppgifter. Den organisatoriska lösningen skulle prövas i två år, varefter den skulle utvärderas och eventuell förändring genomföras.

Det internationella engagemanget inom informationssäkerhetsområdet framhölls i propositionen som viktigt, inte minst på grund av områdets globala natur. Regeringen visade sitt stöd för ambitionen att stärka nät- och informationssäkerheten på europeisk nivå.

1.2 Utredningens direktiv

Utredningen angående vissa frågor om informationssäkerheten i samhället (InfoSäkutredningen) har av regeringen fått i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas. I propositionen 2001/02:158 s. 105 Samhällets säkerhet och beredskap anmälde regeringen sin avsikt att göra en utvärdering av de bedömningar som regeringen gjorde inom informationssäkerhetsområdet. Utredaren fick i uppdrag att följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit myndigheterna i uppgift enligt propositionen. I uppdraget ingick även att lämna förslag till hur OECD:s riktlinjer om säkerheten i nät- och informationssystem kan genomföras i Sverige.

Det ursprungliga direktivet (dir. 2002:103) samt tilläggsdirektiven (dir. 2003:29 och 2004:46) återges i sin helhet i bilaga 1–3.

Utredningens uppgifter enligt direktiv 2002:103 samt tilläggsdirektiv 2003:29 och 2004:46 kan sammanfattas som följer:

Signalskydd

Utredaren skall bedöma behovet av signalskydd i samhällsviktig verksamhet och lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall mot bakgrund av utvecklingen inom informationssäkerhetsområdet föreslå hur signalskyddstjänsten i Sverige skall vara organiserad. Utredaren skall också belysa hur signalskyddsutbildningen skall organiseras och var den skall lokaliseras.

Nationell strategi

Utredaren skall lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas. Den i prop. 2001/02:158 redovisade strategin för informationssäkerhetsarbetet skall utgöra grunden. Utredaren skall utvärdera strategin och om så är befogat, föreslå ändringar. Inom vilka delar av informationssäkerhetsområdet bör staten ha ett särskilt ansvar? Hur skall informationssäkerhetsarbetet finansieras?

Internationell koppling

Utredaren skall göra jämförelser med hur andra länder har hanterat informationssäkerhetsfrågan när det gäller strategi, organisation och andra förhållanden som kan vara relevanta. Utredaren skall överväga hur det kan säkerställas att den nationella strategin för informationssäkerhet möter de krav som ställs via det multinationella samarbete Sverige deltar i, främst inom EU. Utifrån en nationell strategi behöver den nuvarande samordningen av Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet förändras.

OECD:s riktlinjer

I sitt arbete skall utredaren beakta OECD:s riktlinjer för säkerheten i nät- och informationssystem och lämna förslag till hur riktlinjerna kan genomföras i utredarens förslag.

Författningsändringar

Om utredaren finner att det finns ett behov av att föreslå författningsändringar skall utredaren lämna lagtekniskt genomarbetade förslag vid varje rapporteringstillfälle.

Organisationsfrågor

Utredningen skall genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen prop. 2001/02:158 s. 105 Samhällets säkerhet och beredskap, vad avser de bedömningar som regeringen gjorde inom informationssäkerhetsområdet beträffande uppgiftsfördelningen.

Uttolkning av utredningens uppdrag

Utredningens uppgift är inte att en gång för alla lösa frågan om informationssäkerhet. Detta eftersom det inte är en fråga som har någon slutlig lösning. Eftersom utvecklingen på tekniksidan ständigt går framåt måste det i uppgiften att skapa en strategi för informationssäkerhet ligga att skapa långsiktiga, flexibla förutsättningar (även för svensk förvaltning) som kan anpassas efter skiftande behov. Utredningens uppgift och ambition är att dess förslag skall utgöra ytterligare ett steg mot säkrare informationshantering.

I utredningens uppgift ligger att tydliggöra de samverkansprocesser som är nödvändiga för ett effektivt informationssäkerhetsarbete, liksom att klargöra inom vilka delar av informationssäkerhetsområdet staten bör ha ett särskilt ansvar. Utredningen skall även besvara frågan hur informationssäkerhetsarbetet skall finansieras.

Utredningens skall sammanfattningsvis utveckla regeringens strategi för informationssäkerhet ytterligare ett steg. I detta ingår att förmedla insikten att informationssäkerhetsproblematiken inte kan lösas en gång för alla utan att fokus bör läggas på att skapa processer som lär oss att leva med sårbarheter. Utredningens uppgift är också att föreslå hur förutsättningar för olika aktörer att höja sin informationssäkerhet kan grundläggas samt att föreslå medvetna satsningar på samverkansstimulerande åtgärder.

1.3 Det offentliga åtagandet[1]

I Sverige värnar vi om en rad principer som ska garantera att beslut fattas så nära den verksamhet som kommer att påverkas av beslutets innehåll som möjligt. Det gäller ända ner på individnivå, där enskilda aktörer så långt möjligt ges ett avgörande inflytande över beslut som rör deras egen välfärd. Med decentraliserat ansvar och beslutsutrymme följer också ansvar för den egna verksamheten.

Det finns dock verksamheter, funktioner och situationer då enskilda företag och individer inte förmår, eller rimligen kan avkrävas, att axla detta ansvar på egen hand. I vissa fall är det nödvändigt att fatta kollektiva beslut och att flytta över ansvaret till offentliga organ. En diskrepans föreligger mellan vad som är rationellt handlande för en enskild och vad som är rationellt för samhället.

Det finns ett flertal motiv utöver politiska överväganden till offentliga satsningar inom olika områden. Dessa har i stor utsträckning hämtat inspiration ur ekonomiska teorier om statens roll i samhällsekonomin. Sett ur ekonomisk synvinkel kan marknaden hävdas innehålla en del brister, till exempel över- eller underkonsumtion och behov som marknaden inte kan tillgodose på egen hand. Här kan det vara nödvändigt för samhället, genom staten, att intervenera för att skapa balans.

Försvar, rättsväsende, räddningstjänst och vissa delar av infrastrukturen är klassiska exempel på kollektiva nyttigheter. Dessa funktioner kommer alla till godo. Krishantering på samhällsnivå har i grunden samma karaktär som dessa verksamheter. Om det offentliga inte engagerar sig inom dessa områden kan man befara att satsningar som görs blir otillräckliga. Det beror på att medborgarna har svårt att överblicka och värdera de risker som finns för allvarliga kriser eller brister i säkerheten i till exempel den infrastruktur som är avgörande för samhällets funktionsförmåga. Allmänheten har svårt att förbereda sig för egen del om offentliga organ inte gör riskbedömningar och förmedlar resultatet.

Allvarliga kriser, som följer av till exempel brist på säkerhet i infrastruktur, kännetecknas också av att ett stort antal människor och företag samtidigt drabbas av konsekvenserna. Försäkringslös-

[1] Underlag för resonemanget är delvis hämtat ur Ds 1994:53, Motiv för offentliga åtaganden samt SOU 2001:41, Säkerhet i en ny tid, Slutbetänkande från Sårbarhets- och säkerhetsutredningen.

ningar kan därför sällan användas för att fullt ut kompensera de drabbade för de skadeverkningar som uppstår.

Informationssäkerhet, inklusive de krav som måste ställas på säker tillgång till el- och teleförsörjning, är ett område som motsvarar de kriterier som kan uppställas för att det offentliga skall engagera sig i verksamheten. Det offentliga engagemanget bör i första hand gälla den typ av situationer i vilka endast statliga organ kan ta övergripande ansvar för att leda, samordna och prioritera de åtgärder som behövs för en tillfredsställande säkerhet. Det kan gälla situationer som är mycket osannolika, har långtgående konsekvenser för ett stort antal människor och där icke-offentliga aktörer kan ha svårt att på egen hand vidta effektiva åtgärder för att minska skadeverkningar.

Av detta följer inte att offentliga organ bör ta på sig ett generellt finansieringsansvar för de åtgärder som kan krävas för att möta dessa behov. Ett skäl till detta är att skadeverkningarna också av mycket allvarliga brister eller kriser kan begränsas om grundläggande säkerhetsåtgärder vidtas av den som är ansvarig för en verksamhet.

Det är sannolikt inte rationellt för till exempel ett enskilt företag att finansiera en funktion vilken, som extern effekt, kommer även de som inte bidrar till finansieringen till del. En sådan satsning är helt enkelt inte ekonomiskt lönsam. Ett offentligt engagemang inom dessa områden är därför nödvändigt för att ge tillräckliga satsningar. Att det kan vara svårt för en enskild aktör att skapa sig den helhetsbild och den långsiktighet som krävs för vissa beslut, för att de skall fattas på rationella grunder, är ett annat skäl till offentligt åtagande.

Man kan således konstatera att informationssäkerhet på samhällsnivå till vissa delar är en kollektiv nyttighet och därför delvis bör ingå i det offentliga åtagandet. Alla de åtgärder som vidtas för en betryggande säkerhet kan dock inte betraktas som en offentlig angelägenhet. Det finns tvärtom anledning att betona att såväl allmänheten som företag och organisationer har anledning att ta eget ansvar.

1.4 OECD:s riktlinjer

I utredningens uppdrag ingår enligt direktiven att beakta hur OECD:s riktlinjer för säkerheten i nät- och informationssystem kan införlivas i en svensk nationell strategi för informationssäkerhet. ”OECD:s riktlinjer för säkerheten i nät- och informationssystem – på väg mot en säkerhetskultur”, antogs som en rekommendation från OECD-rådet vid dess 1 037:e session den 25 juli 2002.

Riktlinjerna har som mål att:

- främja en säkerhetskultur bland alla deltagare som ett sätt att skydda informationssystem och nät,
- göra deltagarna medvetna om riskerna för informationssystem och nät, om de regler, förfaranden, åtgärder och rutiner som står till buds för att ta itu med dessa risker och om nödvändigheten att införa och tillämpa dessa,
- främja ett ökat förtroende hos alla deltagare för informationssystem och nät och för det sätt på vilket de tillhandahålls och används,
- skapa en allmän referensram som hjälper deltagarna att förstå säkerhetsfrågorna och ta hänsyn till etiska värderingar vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner för säkerheten i informationssystem och nät,
- uppmuntra alla deltagare att samarbeta och utbyta relevant information vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner som rör säkerheten,
- arbeta för att alla som deltar vid utveckling och införande av standarder skall uppfatta säkerhet som ett viktigt mål.

1.5 EU

Det är en naturlig utgångspunkt för utredningen, vilket också är inskrivet i utredningens uppdrag, att göra en internationell utblick och se hur informationssäkerhetsfrågan hanteras utanför Sveriges gränser. Förutom de lärdomar som kan dras av andra länders ställningstaganden i dessa frågor så finns det i olika internationella fora ett pågående samarbete om informationssäkerhetsfrågor. Det arbete som pågår inom EU är härvid av särskilt stor betydelse. Unionen har genom antagande av Lissabonstrategin i början av 2000 satt upp ett tydligt mål; att Europa skall bli den mest konkurrenskraftiga och dynamiska kunskapsbaserade ekonomin i världen. Genom de

därpå följande handlingsplanerna e-Europa 2002 och e-Europa 2005 har ett antal mål med bäring på informationssäkerhet uppställts, vilka Sverige har att förhålla sig till. Detta är förvisso något som förekommer även i samarbete inom andra internationella fora, men det formaliserade och utvecklade sätt på vilket EU-samarbetet bedrivs innebär att dessa mål blir en självklar del av den nationella agendan. Utveckling inom EU med bäring på informationssäkerhet har skett även utanför e-Europas ram.

Ett övergripande mål för Unionen är att skapa, utveckla och upprätthålla den fria marknaden. Den elektroniska handeln har då en roll att spela. Kommissionen presenterade redan 1997 ett meddelande med förslag på åtgärder för att utnyttja e-handelstekniken. En rad initiativ för att främja e-handeln har därefter tagits, vilka i högre eller lägre grad även innehåller regler om informationssäkerhet. Ett exempel är ett direktiv från 1997 som uppställer ett regelverk för att inom gemenskapen säkerställa samtrafik mellan telenät och samverkan mellan tjänster. Bland så kallade väsentliga krav i direktivet kan nämnas att medlemsstaterna skall kunna garantera upprätthållande av nätens integritet, dataskydd etc. För en utförligare beskrivning av den EU-rättsliga utvecklingen samt pågående initiativ på informationssäkerhetsområdet hänvisas till utredningens andra delbetänkande samt till avsnitt 5.2.

Sammanfattningsvis kan konstateras att det EU-rättsliga regelverket innehåller både övergripande initiativ om informationssäkerhet och sektoriella initiativ, där informationssäkerhet utgör en del. Dessa initiativ har Sverige att förhålla sig till i det egna informationssäkerhetsarbetet. En nationell strategi för informationssäkerhet måste därför vara formulerad på ett sådant sätt att den utveckling som sker inom EU kommer in som en naturlig del.

En annan aspekt av EU-samarbetet är det faktum att EU har utvecklats till en organisation med väletablerade institutioner som, i just detta sammanhang, kan jämföras med federala institutioner. Det har därför varit nödvändigt för EU som organisation att utveckla regler för sin egen informationssäkerhet, på samma sätt som sker nationellt. Dessa regler har formaliserats bland annat genom rådets beslut om antagande av säkerhetsbestämmelser 2001. Bestämmelserna är inte bindande för medlemsstaterna utan gäller hos EU:s råd. Emellertid följer av beslutet att också medlemsstaterna skall vidta lämpliga åtgärder, så att det säkerställs att bestämmelserna respekteras av myndigheter och tjänstemän i medlemsstaterna. Man skulle kunna uttrycka det så att Sverige, för

att kunna delta i EU-samarbetet, har att leva upp till de säkerhetsbestämmelser som EU:s institutioner har antagit.

EU-samarbetet har även format terminologin på informationssäkerhetsområdet, vilket utredningen återkommer till nedan.

Sammantaget leder det ovan beskrivna till att det arbete som pågår inom EU på informationssäkerhetens område utgör en grund för det nationella arbetet och är därmed en viktig utgångspunkt för utredningen.

1.6 Definitioner

Utredningen ser det inte som sin uppgift att skapa en ny terminologi för informationssäkerhetsområdet. Däremot är det befogat att slå fast vilka begrepp utredningen utgår ifrån i sitt arbete och motiven till detta. Ett övergripande skäl till att vissa begrepp används är att de i stor utsträckning är vedertagna bland aktörer i såväl privat som offentlig sektor. Det tidigare förhållandet att språkbruket skilde sig åt mellan privat och offentlig sektor, vilket var ett problem såväl ur samverkans- som författningshänseende, har med tiden blivit mindre påtagligt. Det är snarare så, vilket utredningen redogjorde för i sitt andra delbetänkande, att de begrepp som formulerats av inblandade aktörer efter deras specifika behov inte överensstämmer med de av statsmakterna formulerade definitioner som återfinns i rättsliga, administrativa eller finansiella regler.

Utredningen använder det språkbruk som anges i SIS Handbok 550:Terminologi för informationssäkerhet (utgåva 2, 2004). Vad beträffar begreppet informationssäkerhet är begreppet enligt SIS mycket brett och omfattar en mängd underområden som till exempel grundläggande policy, riskhantering samt administrativa och tekniska åtgärder. Informationssäkerhet är enligt SIS definition, vilken alltså har anammats av utredningen, ”säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även spårbarhet och oavvislighet)”. Begreppet innefattar såväl IT-säkerhet som säkerhet i administrativa rutiner. Denna definition av informationssäkerhet skall ställas mot den legaldefinition av begreppet som återfinns i säkerhetsskyddslagen. Enligt säkerhetsskyddslagen skall säkerhetsskyddet förebygga bland annat att uppgifter som omfattas av sekretess och som rör rikets säkerhet, obehörigen röjs, ändras eller

förstörs (informationssäkerhet). Informationssäkerhet i säkerhetsskyddslagens mening omfattar alltså enbart uppgifter som omfattas av sekretess och som rör rikets säkerhet, men oavsett i vilken form uppgifterna finns (på papper, i IT-system etc.). Utredningen konstaterade i sitt andra delbetänkande att det föreligger ett glapp i förståelsen av begreppet informationssäkerhet mellan denna legaldefinition och dess betydelse i vardagligt tal.

Terminologin inom EU på informationssäkerhetsområdet ger stöd för den bredare definition av informationssäkerhet som utredningen använder sig av. Kommissionen definierar i sitt meddelande från 2001 Nät- och informationssäkerhet: förslag till en europeisk strategi (KOM[2001]298) informationssäkerhet som ”förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten (autentisering), integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät”. I rådets säkerhetsbestämmelser slås fast att informationssäkerhet rör skyddandet av uppgifter mot oavsiktligt eller avsiktligt sekretessbrott, förlust av okränkbarheten eller tillgängligheten (det vill säga att förebygga förvanskning, obehörig ändring eller radering samt att åtkomst inte skall nekas den som är behörig). Båda dessa skrivningar överensstämmer i hög grad med utredningens definition. Det man vill uppnå är konfidentialitet, okränkbarhet och tillgänglighet. En viktig likhet är det faktum att begreppet informationssäkerhet inte är kopplat till skyddet av handlingar som omfattas av sekretess. Att kunna garantera tillgänglighet och okränkbarhet (integritet) är viktigt även i fråga om öppna handlingar.

Ett annat begrepp som har visat sig ha grundläggande betydelse för utredningsarbetet är samhällsviktig verksamhet. I diskussionen av vad som utgör det offentliga åtagandet är begreppet återkommande. Enligt utredningens erfarenhet finns dock inte någon generellt vedertagen definition av begreppet. Sannolikt är det så att det finns en mängd olika verksamheter som vid ett givet tillfälle kan vara mer eller mindre viktig för samhället. Staten kan således ha ett ökat intresse av att säkerheten upprätthålls i sådana verksamheter. Det finns därmed ett behov av att vidare definiera vilka kriterier som skall uppfyllas för att en verksamhet eller ett system skall definieras som samhällsviktigt. Utredningen återkommer till detta i avsnitt 4.4.

2 Underlag för utredningens överväganden

2.1 Tidigare betänkande: Delrapport 1: Signalskydd

Signalskyddstjänst var tidigare en egen disciplin, som i stor utsträckning hanterades skilt från kommunikation av information. Den tekniska utvecklingen inom detta område bidrar till att integrera kryptografiska funktioner i informationssäkerhetsprodukter och i dag är signalskyddet integrerat i IT- och kommunikationsutrustningen. Utredningens första delbetänkande innehöll därför inte några förslag inom signalskyddsområdet. Dessa bör formuleras först när övriga delar av informationssäkerhetsområdet har belysts och då vägas in som en del av informationssäkerhetsområdet i det fortsatta arbetet.

Utredningen konstaterade i betänkandet att det finns ett behov av signalskydd även utanför det som lagstiftningsmässigt definieras som totalförsvaret. Möjligheterna att finansiera resurser och kompetens inom totalförsvaret måste vägas mot möjligheterna att tillgodose behoven med kommersiellt tillgängliga system. Utredningen pekade på behov och intresse av samarbete mellan den verksamhet som bedrivs inom totalförsvaret och den inom privat eller kommersiell verksamhet, som motiverar vidare utredning av samverkansmöjligheter. Det har därför också funnits ett behov av att se över gränsdragningar i lagstiftningen, ansvarsförhållanden, organisation etc.

Utredningen utgick ifrån att en svensk anpassning till internationella normer (till exempel de gällande inom EU) avseende signalskydd och hantering av skyddsvärd information, är eftersträvansvärd. En möjlighet syntes vara att utvidga säkerhetsskyddslagens tillämpningsområde till att omfatta även annan skyddsvärd information än den som är hemlig med hänsyn till rikets säkerhet. Med en sådan ordning skulle en större krets av de organ som hanterar skyddsvärd information kunna omfattas av tillämpningsföre-

skrifter eftersom lagens tillämpningsområde även omfattar kommuner, landsting och vissa andra enskilda rättssubjekt.

Ett mindre långtgående alternativ ansågs kunna vara att regeringen föreskriver att särskilda signalskyddsrutiner med mera, skall tillämpas hos de statliga myndigheterna. Inom ramen för den första delrapporten var det dock inte möjligt att närmare analysera frågeställningen. Utredningen ansåg dock att det är angelägna frågor som det var viktigt att särskilt belysa.

De frågor som utredningen beslutade att vidare utreda i det fortsatta arbetet rör organisation, lokalisering och författningsändringar. Då signalskydd av utredningen definieras som en integrerad del av informationssäkerhet i stort, omfattas området i övrigt av de förslag gällande informationssäkerhet som utredningen presenterar.

2.2 Tidigare betänkande: Delrapport 2: Informationssäkerhet i Sverige och internationellt – en översikt

Det offentliga åtagandet

Utredningen slog i sitt andra delbetänkande fast att det är nödvändigt att det offentliga engagerar sig i informationssäkerhetsfrågorna, eftersom satsningarna annars kan förväntas bli otillräckliga. Det är också enbart staten som kan ha den överblick som är nödvändig för att kunna göra adekvata riskbedömningar. Det är dock viktigt att det offentligas engagemang begränsas till de områden eller åtgärder där dess roll är avgörande eller nyttan är så stor att det motiverar offentligt ingrepp. I vissa fall kan det vara befogat att offentliga organ tar ansvar för finansiering och genomförande av säkerhetsåtgärder.

Utredningen redovisade mot denna bakgrund de huvudsakliga funktioner och kontinuerliga arbetsuppgifter för offentliga organ som, utöver det ansvar som följer av ansvarsprincipen och oberoende av dagens organisationsstruktur och funktioner, kunde identifieras inom informationssäkerhetsområdet. Dessa berörde bland annat tydliggörandet av en nationell strategi, att föreslå och förmedla grundläggande regelverk, signalskyddstjänst, att ge råd och information till allmänheten och stöd till myndigheter, särskilda råd och stöd till särskilt viktiga myndigheter eller

avseende särskilt viktiga system och att förebygga, upptäcka, utreda och lagföra IT-relaterad brottslighet.

Utredningen ansåg att det finns flera tänkbara målgrupper för informationssäkerhetsarbetet. De som särskilt nämndes var statlig förvaltning, kommuner och landsting, näringsliv och allmänhet.

De ansvariga statliga myndigheterna befanns ha olika roller, däribland tillsyn, främjande, producent och konsument. Det statliga ansvaret kan utövas på olika sätt. Det kan omfatta till exempel regelstyrning, tillsyn, budgetstyrning eller myndighetsstyrning.

Utredningen konstaterade att informationssäkerhetsarbetet i andra länder har organiserats på principiellt skilda sätt och att arbetsuppgifter, målgrupper, roller och styrinstrument har tolkats och hanterats olika.

Utredningen följde utvecklingen av informationssäkerhetsfrågorna i Sverige och den uppgiftsfördelning som gjordes i propositionen 2001/02:158 Samhällets säkerhet och beredskap. Det låg vid utgivandet av utredningens andra delbetänkande inte i utredningens uppdrag att närmare utvärdera verksamheten, men man kunde konstatera att verksamheten hade kommit igång.

Utredningen konstaterade att det under 2003 förekommit diskussioner rörande gränsdragningsfrågor, dels om relationen mellan de fyra särskilt utpekade myndigheterna, dels om dessa myndigheters relation till andra myndigheter verksamma inom informationssäkerhetsområdet, till exempel Statskontoret, Styrelsen för ackreditering och teknisk kontroll (SWEDAC), Säkerhetspolisen (Säpo) och Försvarsmakten. Oklarheterna om gränsdragning gäller i vissa fall instruktioner för myndigheterna, men framför allt den praktiska uppdelningen av arbetet. Vidare befanns den operativa ansvarfördelningen och samordningen vid krishantering vara oklar. Det framkom också farhågor att utpekandet av särskilt ansvar för vissa myndigheter riskerar att överskugga det ansvar som varje myndighet har inom sitt område. Vissa lagtekniska hinder för verksamheten har också kunnat konstateras.

Utredningen slog fast att informationssäkerhet är, och kommer att vara, en angelägenhet för var och en som hanterar information i någon form. Samtidigt måste arbetet med denna typ av frågor samordnas. Det måste också bedrivas både med långsiktighet och med beredskap i det korta perspektivet.

Analys av kritisk infrastruktur

Analysen av vad som är samhällsviktig infrastruktur är nödvändig för att myndigheternas roller och ansvar skall kunna fastställas.

Utredningen argumenterade för att utgångspunkten för fastställande av ansvar, åtgärder, finansiering, m.m., bör vara *funktionsorienterad*. Tidigare har utgångspunkten för informationssäkerhetsarbetet varit *situationsberoende* i meningen att ansvar varit beroende av för i vilken situation som informationssäkerheten varit viktig. I första hand har uppdelning skett i termer av informationssäkerhet i fred respektive under höjd beredskap och krig. Således har till exempel Statskontoret och Krisberedskapsmyndigheten likartade eller jämförbara uppgifter rörande informationssäkerhet, men för olika situationer.

Utredningen menade att upprätthållande av kritisk infrastruktur bör vara utgångspunkten för vilket ansvar staten har för informationssäkerheten.

Begrepp och definitioner

Utredningen fokuserade på legaldefinitioner som skulle kunna koppla samman de övergripande begreppen och definitionerna med de tekniska och administrativa som redan finns etablerade. Utredningen ansåg det viktigt att skapa en grund för tydligare författningar samt att öka spårbarheten inom informationssäkerhetsområdet och därmed möjligheterna att förankra begrepp och definitioner hos alla aktörer och användare.

Ett problem som utredningen pekade på var att de begrepp som skapas för att fungera i rättsliga sammanhang inte alltid harmonierar med de begrepp som utvecklas och används av ansvariga för forskning och utveckling, producenter, leverantörer, systemkunniga, tekniker med flera. Nuvarande regelverk om informationssäkerhet är endast allmänt hållna och speglar knappast det faktum att en mycket stor del av informationshanteringen i samhället inte längre föreligger i traditionell fysisk form. Utredningen menade att begrepp och definitioner som rör informationssäkerhet måste konkretiseras ytterligare för att kunna tjänstgöra som verktyg och att regelverket i högre grad bör anpassas till hantering av handlingar i IT-system.

Utredningen hänvisade härvid till att de begrepp som används i SIS Handbok 550: Terminologi för informationssäkerhet, som är väl förankrade internationellt och nationellt, liksom BITS (Basnivå för IT-säkerhet), som utgör ett intressant exempel på hur informationssäkerhetsarbetet kan konkretiseras med stöd av precisa författningar.

Internationell koppling

Enligt utredningen föreföll det som att EU (och OECD) har bättre anpassade bestämmelser och tydligare visioner för informationssäkerhetsarbetet än Sverige. Några undantag från EU:s säkerhetsbestämmelser har inte gjorts från svensk sida. Bestämmelserna reglerar hantering av sekretessbelagda EU-uppgifter. Enligt artikel 2 i beslutet skall medlemsstaterna vidta lämpliga åtgärder så att det vid hantering av sekretessbelagda EU-uppgifter säkerställs att bestämmelserna respekteras av medlemsstaternas myndigheter och i deras lokaler. Även om bestämmelserna bara omfattar sekretessbelagda EU-uppgifter skulle de kunna utgöra en utgångspunkt för utredningens fortsatta överväganden. Med den grundläggande definitionen av informationssäkerhet inom EU (”uppgifter som lagras, bearbetas eller överförs i elektronisk form”) som utgångspunkt skulle bestämmelser kunna konkretiseras utifrån den administrativa och tekniska hierarki som utarbetats inom SIS-projektet. Utredningen pekade på regeringens möjligheter att genom den delegerade normgivningskompetensen utfärda förordningar för att styra all statlig verksamhet. Det skulle således vara möjligt att samla bestämmelser om informationssäkerhet på motsvarande sätt som redan görs för krig och krigsfara, genom BITS. I detta sammanhang skulle begrepp och definitioner kunna utvecklas.

Författningar

Utredningen erfor att flera myndigheter upplevde att begreppet rikets säkerhet i 2 kap. 2 § sekretesslagen (1980:100) har ett för snävt tillämpningsområde. Mycket av för samhället viktig verksamhet faller utanför säkerhetsskyddslagen (1996:627) eftersom den inte rör rikets säkerhet enligt dagens tolkning av begreppet. Begreppet bör enligt dessa myndigheter utvidgas till att inkludera

även de vidare aspekter som borde ingå i ett begrepp för nationell säkerhet. Till exempel borde begreppet inkludera ekonomisk säkerhet och attraktionskraft och handelsstatus. Sverige bör dock inte gå längre i sin tolkning av när inskränkningar är tillåtna än vad som accepteras av den Europeiska domstolen för de mänskliga rättigheterna.

Utredningen konstaterade att det kunde finnas anledning att analysera säkerhetsskyddslagen (1996:627) närmare i det fortsatta arbetet. Med hänsyn till den teknikutveckling som skett och särskilt med hänsyn till den omfattande användningen av Internet och e-post finns det, enligt utredningen, anledning att i det fortsatta utredningsarbetet ta ställning till om det behövs en mer genomgripande översyn av lagar och förordningar som har relevans för dessa frågor. För det fall att utredningen kom fram till att det skall formuleras regler för informationssäkerhet med utgångspunkt i den bredare definition som utredningen har använt sig av, måste utredningen ta ställning till hur detta skall förhålla sig till säkerhetsskyddslagens regler om informationssäkerhet i den mer begränsade betydelsen att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Det internationella perspektivet konstaterades vara av stor betydelse både vad gäller säkerhetsskyddsklassning och brottsförebyggande och lagförande av IT-relaterad brottslighet.

Incidentrapportering

Att rapporter om IT-incidenter som lämnas till en myndighet (till exempel SITIC-funktionen på Post- och telestyrelsen) blir allmänna handlingar enligt offentlighetsprincipen i och med att de inkommer till myndigheten var vid tiden för inlämnande av utredningens andra delrapport ett problem. Detta problem uppmärksammades med anledning av inrättandet av funktionen för IT-incidentrapportering. Eftersom offentliggörande av informationen kan vara till förfång för den organisation som lämnat in den, är en förutsättning för exempelvis SITIC:s bedrivande av sin verksamhet att det finns möjlighet att hemlighålla uppgifterna. Under 2002 lämnade Post- och telestyrelsen ett förslag till regeringen om modifiering av sekretesslagen, vars syfte var att skapa förutsättningar för SITIC att sekretessbelägga incidentrapporter från i princip samtliga rapportörer,

inte enbart från så kallade bevakningsmyndigheter. Utredningen uttryckte sin avsikt att återkomma i frågan.

Kompetensförsörjning

Utredningen slog fast att det föreligger ett generellt behov av att öka medvetenheten om sårbarheter och risker på alla nivåer i samhället. Dessutom finns det ett behov av att stärka beställarkompetensen hos ägare av samhällsviktig infrastruktur. Företeelsen outsourcing, att lägga verksamhet på entreprenad, ökar ytterligare behovet av beställarkompetens. Behovet av kryptokompetens i samhället är stort och växande. Kompetenskraven har höjts kraftigt under senare år. Utredningen avsåg att återkomma med förslag till åtgärder för hur detta behov skall kunna tillgodoses.

För att täcka de behov av utbildning och medvetandegörande som ansågs finnas, föreslog utredningen en rad åtgärder. Säkerhetsinslag i utbildningen redan på grundskolenivå är ett sätt att på bred front öka medvetandet. Beträffande högskolenivå angav utredningen sin avsikt att vidare belysa tillgången till säkerhetsinriktade ämnen inom bland annat tekniska och ekonomiska utbildningar. Som en del i samhällets säkerhetsförebyggande arbete finns skäl att överväga att bygga in rekommendationer om inslag av utbildning om sårbarhet och säkerhet som en normal del i grundutbildningarna för till exempel civilingenjörer, civilekonomer och i vissa andra akademiska examina.

En metod för att ytterligare utveckla beställarkompetens kan vara att använda gemensamma standarder för informationssäkerhet. En standard innehåller en uppsättning styrmedel och baseras på god praxis. Den kan vara avsedd för de flesta situationer där informationssystem utnyttjas, såväl inom myndigheter som inom näringsliv. Utredninges angav att man avsåg att värdera huruvida en mera generell användning av informationssäkerhetsstandard är en bra och resurseffektiv metod för att utveckla beställarkompetens samt en gemensam nivå vad gäller informationssäkerhet.

Den offentliga verksamheten måste på ett aktivt sätt ta tillvara den säkerhetskompetens och den snabba utveckling som finns inom den privata sektorn. Det är inte en uppgift för den offentliga sektorn att tillgodose behovet av leverantörskompetens utan detta bör främst ske genom det utbud som utvecklas på den privata marknaden.

Utredningen konstaterade dock att i den mån marknaden inte är tillräckligt stor eller av någon annan anledning befinnes olämplig, måste staten kunna gå in. När det gäller infrastruktur och informationssystem som är nationellt samhällskritiska, har staten ett särskilt ansvar. Det är därför av nationellt intresse att tillgodose samhällets behov av leverantörskompetens inom området.

Utredningen redovisade sin avsikt att särskilt belysa möjligheterna till kompetensutveckling genom en mera generell användning av revisionsinstrumentet inom områdena informationssäkerhet och IT-säkerhet.

Integrering av informationssäkerhet och signalskydd

Signalskyddet i Sverige har historiskt haft en stark koppling till totalförsvaret (se delbetänkande 1 om signalskydd). Behoven av att skydda information har varit helt knutna till sekretesslagstiftningen. I dag är behoven delvis annorlunda. Det finns ett behov av att skydda information även om den inte är hemlig i enlighet med sekretesslagen (1980:100). Signalskydd bör därför ses som ett medel för att åstadkomma en bättre informationssäkerhet och bör vara en naturlig del i informationssäkerhetsarbetet även utanför totalförsvarsverksamheten.

Utredningen kunde konstatera att civila myndigheter med flera i allt större omfattning begär stöd i signalskyddsfrågor även för hantering av skyddsvärd information som inte omfattas av sekretess.

Inom det internationella samarbetet har Sverige hävdat sig väl inom signalskyddsområdet och ofta uppskattats för sin kompetens. Utredningen konstaterade att en kvalificerad resurs för granskning och i tillämpliga fall kryptogodkännande av svensktillverkade produkter för internationella organisationers behov dock är nödvändig för att upprätthålla Sveriges goda internationella anseende.

Försvarsmakten utövar rollen som National Communication Security Agency (NCSA) genom Totalförsvarets signalskyddssamordning (TSA). Något formellt beslut har dock inte tagits i denna fråga. Utredningen ansåg att det finns ett behov av att tydliggöra denna roll på ett bättre sätt.

Samordning av det internationella agerandet

Målet för det svenska agerandet på den internationella arenan är att få genomslag för svenska intressen. För att uppnå detta är det viktigt att hänsyn tas till överordnade svenska intressen, och att utgångspunkten för vårt internationella agerande utgörs av en gemensam svensk ståndpunkt. Detta gäller på alla nivåer – regeringen, Regeringskansliet och myndigheter, samt i förekommande fall också för berörda privata aktörer.

Utredningen konstaterade att det finns ett stort behov av samordning mellan olika aktörer. Med en väl genomarbetad och förankrad nationell strategi och en tydlig arbetsfördelning såväl inom Regeringskansliet som mellan myndigheterna bör de befintliga verktygen, det vill säga gemensam beredning, regleringsbrev och myndighetsinstruktioner, vara tillräckliga för att hantera såväl förutsedda som snabbt uppkomna frågor. Utredningen menade däremot att det kan finnas skäl att lägga större vikt vid de internationella frågorna när myndigheternas instruktioner och regleringsbrev ses över.

Finansieringsaspekter

Säkerhet måste ses som intäktsskapande eller kostnadsbesparande. Till exempel är konceptet 24-timmarsmyndighet[1] baserat på flera kvalitativa tjänster till medborgarna till lägre kostnader. Informationssäkerheten berör alla verksamheter och ligger inom varje enskild organisations ansvar. Informationssäkerheten måste lösas i det dagliga arbetet och i den ordinarie organisationen. Därför bör också säkerhetslösningarna finansieras inom de normala finansieringsramarna för verksamheten. Utredningen gjorde bedömningen att kostnaderna, alternativt de negativa effekterna, riskerar att bli avsevärt större om inga åtgärder vidtas.

I den offentliga förvaltningen skall kostnaderna med anledning av de föreslagna åtgärderna redovisas i samband med årsredovisningen. Åtgärderna skall genomföras och finansieras inom tilldelade budgetramar inom respektive myndighetsansvar. När så är tillämpligt kan åtgärder samfinansieras mellan offentlig och privat sektor.

[1] Strategiskt arbete med att utveckla en sammanhållen elektronisk förvaltning drivs av Statskontoret.

Inom Utgiftsområde 6 Försvar samt beredskap mot sårbarhet sker för närvarande en översyn av finansieringsprinciperna för anslaget 6:5 Civilt försvar. Utredningen avsåg följa översynen av dessa principer.

Utgångspunkter för en nationell informationssäkerhetsstrategi

Utredningen konstaterade att en nationell informationssäkerhetsstrategi bör ha ett långsiktigt, framåtblickande perspektiv, som kan ligga till grund för handlingsplaner och åtgärder på två till tre års sikt. Strategin bör vända sig till myndigheter, näringsliv och organisationer, men även till enskilda användare, då de flesta i dag är anslutna till olika lokala, nationella eller internationella informationstjänster. Utredningen redovisade några utgångspunkter som den ansåg borde kunna ligga till grund för det fortsatta arbetet.

Strategin bör inriktas mot att kunna:

- ligga till grund för politiska beslut och prioriteringar inom informationssäkerhetsområdet, och
- förbättra samordningen av samhällets informationssäkerhetsarbete

Strategin bör:

- bidra till att reducera sårbarheten och uppnå en effektiv risknivå i samhällets olika informationssystem och kritiska infrastruktur
- öka och fördjupa tilliten till informationstekniken, ligga till grund för trygg elektronisk kommunikation i privat och offentlig sektor samt säkra pålitliga nättjänster från offentlig sektor.

De överordnade målen för informationssäkerheten sammanfattades av utredningen i några punkter, utifrån ett verksamhetsorienterat perspektiv:

- Infrastruktur: Samhällets infrastruktur för informationstjänster skall vara robust och säker i förhållande till de funktioner den utför. Kritiska informationssystem skall vara så säkra att en skada inte får större verkningar än som kan anses acceptabla.

- Verksamhet: Det skall byggas en säkerhetskultur runt användandet och utvecklingen av IT i Sverige. Informationssäkerhet skall vara en central faktor vid användandet av IT i Sverige.
- Medborgare: Sverige skall ha en allmänt tillgänglig samhällsinfrastruktur för elektroniska signaturer, autentisering av avsändare av elektronisk information samt säker överföring av känslig information.
- Styrning: Regelverk som berör informationssäkerhet skall tillhandahållas och vidareutvecklas på ett samordnat och för användarna enkelt och översiktligt sätt.
- Utbildning: Det skall finnas möjligheter till utbildning inom informationssäkerhetsområdet för alla målgrupper.
- Agerande: Den informationssäkerhet som byggs upp skall stödjas av möjligheter till ingripande vid hot, incidenter, angrepp eller IT-relaterad brottslighet.

2.3 Centrala frågeställningar

I utredningens andra delbetänkande ”Informationssäkerhet i Sverige och internationellt – en översikt”, identifierade utredningen ett antal frågeområden som man aviserade sin avsikt att återkomma till i slutbetänkandet. Detta är områden där tiden inte har varit mogen för slutligt avgörande. Frågeområdena har tjänat som avstamp och ledning i utredningens vidare arbete.

Organisationsfrågor

Utredningen konstaterade utifrån det underlag den fick del av att informationssäkerhetsfrågorna var olika väl förankrade inom olika verksamhetsområden. Av den anledningen ansåg utredningen att det var nödvändigt att sträva efter en ytterligare kompletterad bild av informationssäkerhetsarbetet på den nationella nivån. Utredningen avsåg fortsätta följa arbetet vid de fyra myndigheter som genom proposition 2001/02:158 fått särskilda uppgifter på informationssäkerhetsområdet.

Utredningen angav i delbetänkande två sin avsikt att vidare studera den samverkan som finns mellan privat och offentlig sektor, vilka ytterligare behov samt vilka effekter samverkan kan ha.

Internationell koppling

Utredningen angav i sitt andra delbetänkande att man avsåg behandla de internationella aspekterna utförligare i slutbetänkandet. Det internationella underlaget skulle på ett tydligare vis användas som jämförelseunderlag i den övergripande analysen. Detsamma gällde informationssäkerhetsfrågorna inom EU, som också skulle få en mer framträdande placering i slutbetänkandet.

Författning

Utredningen konstaterade att ett flertal myndigheter pekade på problem med hanteringen av uppgifter som omfattas av sekretess men som inte rör rikets säkerhet och som därmed faller utanför säkerhetsskyddslagens tillämpningsområde. Detta gäller till exempel skydd av kritisk infrastruktur. Sekretess vid IT-säkerhetsanalyser och incidentrapportering är ett annat problem. Myndigheterna pekade på att detta kan få till konsekvens att rapporter inte upprättas eller inte lämnas vidare i tillräcklig utsträckning.

Med hänsyn till denna problematik och den omfattande användningen av Internet och e-post konstaterade utredningen att det fanns ett behov av att ytterligare se över lagar och förordningar med relevans för dessa frågor.

Kompetens

Utredningen avsåg att skaffa sig en uppfattning om utbudet av utbildningar inom informationssäkerhet och värdera kvaliteten på dessa. En belysning av tillgången på säkerhetsinriktade ämnen inom en rad utbildningar ansågs befogad, liksom att överväga om det finns anledning att bygga in rekommendationer om inslag av utbildning om sårbarhet och säkerhet som del i grundutbildningen för vissa akademiska examina. Särskild uppmärksamhet avsåg man lägga på mötet mellan teknik och juridik. Utredningen angav också som ambition att skaffa sig en uppfattning om inriktning och omfattning av dagens forskning inom informationssäkerhet samt att värdera behovet av ytterligare stimulans. Områden som kräver ökad kompetens är bland andra avtals- och upphandlingsfrågor, något som blir ytterligare aktuellt då fenomenet outsourcing ökar. Inom kryptoområdet har kompetenskraven höjts och utredningen

avsåg därför redovisa förslag till åtgärder för att tillgodose detta behov.

Utredningen angav också att man hade för avsikt att särskilt belysa möjligheterna till kompetensutveckling genom en mera generell användning av revisionsinstrumentet inom områdena informationssäkerhet och IT-säkerhet.

Standarder

Utredningen uttryckte avsikten att värdera huruvida en mer generell användning av informationssäkerhetsstandard utgör en bra och resurseffektiv metod för att skapa en grundnivå för informationssäkerhet samt för att utveckla beställarkompetens. Ett alternativ som utredningen såg var att istället för införandet av viss standard, föreslå revisionskrav. Utredningen angav också att man avsåg följa uppbyggnaden av en certifieringsfunktion vid Försvarets materielverk.

Signalskydd

Utredningen konstaterade att det finns behov av att på ett bättre sätt tydliggöra rollen som National Communication Security Agency (NCSA). I dag är det i praktiken Försvarsmakten som genom Totalförsvarets signalskyddssamordning (TSA) har denna roll. Detta trots att något formellt beslut att så skall vara fallet inte har tagits.

Utredningen konstaterade vidare att det sker en eftersläpning av signalskyddsutvecklingen och att en anledning till detta är den organisatoriska placeringen. Det innebär att en avvägning sker mot Försvarsmaktens övriga resurser, då det i dag inte finns medel särskilt avsatt för denna verksamhet. Utredningen skrev att det är viktigt att Sveriges anseende inom detta område upprätthålls genom väl avvägda satsningar och att man därför skulle följa utvecklingen inom dessa frågor.

2.4 Kontakter i övrigt

I syfte att fördjupa underlaget har utredningen genomfört dialoger med berörda myndigheter, Sveriges kommuner och landsting samt med företrädare för näringslivet inom området. Dialogerna med

berörda myndigheter har haft huvudsyftet att ytterligare belysa de frågeställningar som FOI har tagit upp i sitt underlag för utvärdering av uppgiftsfördelningen inom informationssäkerhetsområdet (FOI-R-1369-SE). Organisationsfrågorna har således varit centrala i detta sammanhang. Utredningen återkommer till dessa frågor i slutbetänkandet september 2005.

Som komplement till dessa dialoger har dessutom ett antal seminarier genomförts, där frågor om informationssäkerhetsarbetet inom näringslivet och berörda myndigheter har kunnat belysas ytterligare. En scenarioövning med utredningens experter, sakkunniga samt ytterligare myndighetsrepresentanter genomfördes den 4 oktober 2004. Genom sammansättningen av deltagare ansågs förutsättningarna goda att få frågorna belysta ur ett myndighetsperspektiv. Ytterligare en scenarioövning med samma spelupplägg genomfördes den 15 november 2004. Denna gång med representanter för näringslivet.

2.4.1 Nämnden för e-förvaltning

Nämnden för elektronisk förvaltning, e-nämnden, inrättades den 1 januari 2004. Nämndens uppgift är att stödja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte mellan myndigheter och mellan myndigheter samt enskilda. Detta skall ske genom att nämnden beslutar om de standarder eller liknande krav som skall vara gemensamma för det elektroniska informationsutbytet för myndigheter under regeringen. Nämnden skall vidare bistå med information och utarbeta riktlinjer samt verka för att det på informationsteknikmarknaden tillhandahålls tjänster och produkter till stöd för elektroniskt informationsutbyte.

Nämnden har möjlighet att utfärda såväl bindande föreskrifter som rekommendationer i form av riktlinjer och vägledningar. Arbetet bedrivs i projektform genom att nämnden ger uppdrag till andra myndigheter att bedriva arbete på olika områden. Nämndens uppgifter är fastställda i förordning (2003:769) med instruktion för Nämnden för elektronisk förvaltning och i förordning (2003:770) om statliga myndigheters elektroniska informationsutbyte. Statskontoret ansvarar för nämndens kansli.

Utredningen har tagit del av nämndens arbete genom en av utredningens experter. Se även avsnitt 7.8.

2.4.2 Sveriges kommuner och landsting

En stor del av samhällets informationssäkerhetsarbete bedrivs i kommuner och landsting. I en strategi för informationssäkerhet är det därför viktigt att detta faktum beaktas och att utredningen beskriver de problem kommuner och landsting upplever inom informationssäkerhetsområdet. Utredningen betonar behovet av gemensamma lösningar samt behov av ett bättre kapacitetsutnyttjande för att uppnå ett informationssäkerhetsarbete som alla parter vinner på. Tillit och förtroende inom informations- och kommunikationsområdet är nödvändigt för att ny teknik skall användas mer. Kommunerna uppvisar stora olikheter vad gäller antal invånare, förutsättningar och behov. Variationen i såväl användande av IT, som val av teknik och säkerhetslösningar är i dag stora. Den mest framkomliga vägen förefaller därför vara att från statligt håll föreslå målsättningar för informationssäkerhetsarbetet och överlåta beslut om hur dessa skall uppnås till respektive kommun och landsting.

Sveriges Kommuner och Landsting lyfter fram några frågor som särskilt angelägna i dag: behovet av en långsiktig lösning kring e-legitimation/certifikat, fortsatt utveckling av en obruten vårdkedja, stöd för risk- och sårbarhetsanalyser samt ökad samverkan på alla nivåer.

E-legitimationer och certifikat

Dagens modell för hantering av elektroniska legitimationer och certifikat har visat sig ha egenskaper som i vissa fall snarare hämmar än främjar utvecklingen. Detta beror bland annat på att den bygger på att kontroller av certifikat bekostas via en transaktionsbaserad modell. Detta gör att de kommuner eller landsting som utvecklar e-tjänster ser risker för att kunna få stora och okontrollerbara utgifter.

Affärsmodellen bygger i huvudsak på att myndigheten betalar för varje gång man kontrollerar en e-legitimation eller underskrift. Det finns alternativ som innebär fast pris per månad eller år men kommuner och landsting ser bekymmer med att inte kunna styra över medborgarnas användning och helt få kontroll över kostnaderna.

Dagens lösning på området främjar inte utvecklingen av e-förvaltningen. Kommuner och landsting efterfrågar därför en nationell lösning med ett större statligt ansvarstagande.

Sammanfattningsvis betyder detta att verksamheter med få men stora transaktioner – till exempel självdeklaration via nätet och Centrala Studiestödsnämnden (CSN) – får kostnader som är hanterliga medan den dagliga verksamheten i en kommun kan leda till okontrollerbara och mer kännbara kostnader.

Obruten vårdkedja

Carelink[2] arbetar tillsammans med Landstingen med att ta fram samverkansformer och lösningar för att utveckla de informations- och kommunikationssystem som är knutna till vården. Carelink förvaltar och utvecklar sedan 1 januari, 2001 Sjunet, den nationella infrastrukturen för vård och omsorg.

Sjunet är ett VLAN (Virtuellt LAN). Samtliga landsting, ett antal kommuner, ett antal privata vårdgivare inkl Praktikertjänst och Capio, Skatteverket samt ett tjugotal leverantörer, inklusive Apoteket, är i dag anslutna till Sjunet.

Risk- och sårbarhetsanalyser

Det är angeläget att informationssäkerhetsfrågor tas upp i de risk- och sårbarhetsanalyser som genomförs i kommuner och landsting. Det gäller såväl verksamhetsrelaterade risker som eventuella integrerade informationssäkerhetsproblem. Delvis är detta en resursfråga. De mindre kommunerna har varken ekonomiska eller personella resurser att göra särskilda informationssäkerhetsanalyser. Framtagande av checklistor anpassade till olika verksamheter kan vara en väg att underlätta ett sådant arbete.

Frågeställningen måste hanteras genom att nyttan av att inkludera informationssäkerhetsfrågor i risk- och sårbarhetsanalyser lyfts fram. Sveriges Kommuner och Landsting har medverkat i två stödprojekt riktade till kommunerna i samband med statliga satsningar: projektet Infrabas som var en del av ITiS –satsningen (IT i Skolan) samt ett pågående projekt kopplat till bredbandsutbyggnaden. Erfarenheterna av denna form av stöd till kommunerna är mycket goda.

[2] Carelink bildades i december 2000 av Landstingsförbundet, Svenska kommunförbundet, Föreningen Vårdföretagarna (f.d. Privatvårdens Arbetsgivarförbund) och Apoteket AB. Socialstyrelsen stöder verksamheten genom ett samverkansavtal.

Stöd och inspiration till att genomföra lokala övningar, där effekter av till exempel konsekvenser av internt genererat databortfall (och inte, som vanligtvis, skadekonsekvenser från en extern kris eller olycka) övas, är efterfrågat. Sådana övningar är ett sätt att öka medvetenheten på bred front.

Kompetensfrågor

Informationssäkerhetsfrågorna måste hanteras som en integrerad del av skolans verksamhet. Utrymmet för särskilda insatser är i dag mycket begränsat. Frågor som inte hanteras inom ordinarie läroplan löper stor risk att aldrig tas upp. Pedagogiken är viktig och bör utgå från ”naturliga” drivkrafter hos användare. Det är också angeläget att dessa frågor lyfts in i grundutbildningen.

Samverkan mellan stat och kommuner

Ur kommun och landstingsperspektiv är det önskvärt att oklarhet kring olika myndigheters roller reds ut. En bättre samordning av statens insatser efterfrågas. I dag är det inte ovanligt att flera myndigheter närmar sig kommunerna med frågor som tangerar varandra, vilket medför såväl merarbete som ökade kostnader för kommunerna. Det finns ett stort behov av förbättrad samverkan mellan staten och kommuner och landsting. Bredbandsutbyggnaden är ett gott exempel på samverkan där lokala förutsättningar och drivkrafter har beaktats av staten.

Sveriges Kommuner och Landsting har i dag ett förbundsövergripande projekt, ”e-förvaltningsprojektet” som har till uppgift stödja kommuner och landsting i deras strategiska arbete med att utveckla en sammanhållen elektronisk förvaltning (24-timmarsmyndighet). Detta arbete sker i nära kontakt med de myndigheter och departement som hanterar dessa frågor.

2.4.3 Näringsliv

Eftersom näringslivet är en heterogen grupp företag med skiftande förutsättningar och mål kan de inte till fullo antas ha sammanfallande behov och krav på informationssäkerhet. Det är viktigt att hålla detta i åtanke, i sammanhang där näringslivet nämns. Utred-

ningen har eftersträvat en inblick i vilka förväntningar representanter för olika delar av näringslivet har på utvecklingen av informationssäkerhet och hur de ser på de statliga åtgärder som hittills prövats. Enligt utredningens direktiv skall den strategi som formuleras omfatta hela samhället. Att i en strategi övervägande fokusera på statlig förvaltning leder fel. Utredningen har vid ett flertal tillfällen sammanträffat med representanter från olika delar av näringslivet. Kontakt med de representanter som utredningen träffat har sökts bland annat via Svenskt Näringsliv och Näringslivets Säkerhetsdelegation. Utredningen har samtalat med olika representanter, dels under sammanträden tillsammans med utredningens experter och sakkunniga och dels under en scenarioövning.

2.5 Utredningens slutsatser av inhämtat underlag

De genomförda dialogerna och seminarierna har bidragit till att bekräfta bilden av behov, möjligheter och problem inom informationssäkerhetsområdet. Tillsammans med de iakttagelser som utredningen redovisat i delrapport 2 utgör dessa ett bra underlag för de överväganden som redovisas i de följande avsnitten.

Ett första viktigt konstaterande är att staten har i stort sett samma problembild att hantera som den som redovisas av Sveriges kommuner och landsting. Det handlar om gränssnittet mellan myndigheter och medborgare, om tillit och förtroende och möjligheter till ökad delaktighet i den offentliga verksamheten samt om ökad tillgänglighet till information med bevarad integritet och trygghet. En utveckling av informationsförsörjning i alla dessa avseenden förutsätter att ett antal säkerhetsproblem löses. Vidare har staten och kommunerna en i allt väsentligt likartad struktur, såväl politiskt som organisatoriskt. Förutsättningarna för samverkan inom staten respektive mellan kommunerna företer många likheter.

Ett andra viktigt konstaterande är att, även om offentlig sektor och näringslivet i många avseenden delar problemen med bristande informationssäkerhet, skiljer sig förutsättningarna i fråga om struktur, organisation och möjligheter till samverkan. Inom näringslivet finns inte förutsättningar för central styrning eller representativ samverkan så som är vanligt inom offentlig sektor. Näringslivets motsvarighet kan möjligen återfinnas inom branscher, där staten ställer vissa gemensamma krav genom lag eller motsvarande, till exempel inom bankväsendet. Ofta uppträder varje företag för sig

och agerar på en konkurrensutsatt marknad. Samverkan är därför inte alltid möjlig eller ens önskvärd.

En tredje iakttagelse från seminarierna är att informationssäkerhet samtidigt kan ses som ett gemensamt, tvärsektoriellt problem och som ett individuellt problem knutet till den egna, sektorsspecifika verksamheten. Detta leder till att olika lösningar sannolikt måste sökas parallellt. Det kan således handla om att finna vägar att öka informationssäkerheten som en integrerad del av respektive verksamhet och att utveckla samverkan inom respektive branscher och sektorer i detta syfte. För detta krävs sannolikt en tydligare uttalad ansvars- och arbetsfördelning inom respektive sektor av samhället. Men det har även framkommit att det finns klara begränsningar i vad som kan uppnås genom sådana individuella lösningar. Det finns således ett antal kvalificerade frågeställningar inom informationssäkerhetsområdet, både vad avser komplexitet och möjliga konsekvenser eller skador av brister i informationssäkerheten. Dessa problem är av tvärsektoriell, gemensam natur och förutsätter ett annat angreppssätt på styrning och organisation. En förutsättning för detta är bland annat att gränserna mellan det offentliga åtagandet och det privata tydliggörs.

En fjärde iakttagelse är att det redan i dagsläget finns ett utvecklat samverkansmönster mellan stat och berörda företag inom vissa verksamhetsområden vilket kan tjäna som förebild för en bredare och fördjupad samverkan i informationssäkerhetsfrågor på flera områden.

Utredningen återkommer till de organisatoriska frågorna i sitt slutbetänkande. Dialogerna med berörda myndigheter och olika företrädare för näringslivet utgör en viktig del av underlaget inför för utredningens överväganden om uppgiftsfördelningen inom informationssäkerhetsområdet.

3 Behovsbilden

De flesta verksamheter är i dag beroende av information för att kunna fungera. Beroendet av fungerande informations- och kommunikationsverktyg för att informationen skall kunna hanteras effektivt innebär nya utmaningar. Utredningen konstaterade i sitt andra delbetänkande att den tekniska komplexiteten ökar och att möjligheterna att ersätta IT-system med manuella funktioner i många fall har försvunnit. Denna utveckling bidrar till ett ökat beroende av IT för den dagliga verksamheten, styr- och reglerfunktioner, ekonomiska och administrativa funktioner med mera. Beroendet av tekniken, som ökar inom samtliga sektorer i samhället, och därpå följande förändringar i rutiner och handhavande skapar en mängd behov. Nya behov som uppkommer genom utvecklingen kan vara en statlig angelägenhet men kan också vara nya omständigheter för respektive verksamhetsansvarig eller användare att beakta och hantera.

Behoven inom informationssäkerhetsområdet skiljer sig åt mellan olika aktörer. Behov och möjligheter kan dessutom ses ur flera vinklar: ur *verksamhetssynpunkt* och ur *säkerhetssynpunkt*. I verksamhetsansvaret ingår kravet på informationssäkerhet, vilket innebär att en verksamhetsanpassad säkerhetsnivå skall uppnås inom ordinarie ekonomiska ramar. Vare sig uppgiften är hälso- och sjukvård eller annan verksamhet, är respektive verksamhetsansvarig i någon mening ansvarig för resultatet. Detta styrs på olika sätt inom privat och offentlig sektor och säkerhetsarbetet utgör en integrerad del av verksamheten. Den IT-relaterade hotbilden innebär dock att flera aktörer kan vara drabbade av samma problem och att det finns åtgärder som skulle kunna vara till nytta för flera av dem som utsatts.

Gemensamt för flertalet aktörer är behovet av att minska sårbarheten i de informations- och kommunikationssystem som är viktiga för den egna verksamheten. Alla sårbarheter kan dock inte

byggas bort. Därför måste bland annat säkerhetsmedvetandet ökas för att kompensera för kvarstående sårbarhetsproblem. Bedömningen av sårbarheter bör göras utifrån välgrundade sårbarhets- och riskanalyser, vilka kan indikera vilken nivå säkerheten bör ligga på.

3.1 Behov, möjligheter och problem ur verksamhetssynpunkt

Allt fler verksamheter kräver hög informationssäkerhet för att kunna bedrivas på ett korrekt sätt. Informationssäkerhet kan vara huvuduppgiften eller en sekundär uppgift. För den verksamhetsansvarige utgör informationssäkerheten i de flesta fall ett av flera krav som skall uppfyllas i verksamheten. Informationssäkerhet är inte en åtgärd vid extraordinära händelser, utan ett vardagskrav för god funktion. Många verksamheter är i ökande grad beroende av elektroniska kommunikationstjänster. Dels för överföring av olika typer av information inom den egna organisationen och dels för kommunikation med externa aktörer eller funktioner. Information kan utgöra verksamhetens huvudsakliga tillgång medan andra organisationer kan vara beroende av stödfunktioner vars informationssäkerhet det måste gå att ställa höga krav på.

Olika aktörer – som offentlig sektor, privat sektor och med–borgare – har olika behov på informationssäkerhetsområdet, men också skiftande ansvar och skyldigheter. Alla aktörer har inte heller samma möjligheter eller incitament att bidra till informationssäkerhet utanför den egna verksamheten.

Samhällets medborgare har ett behov av att kunna lita på funktionaliteten och förutsägbarheten i de informationstjänster som de är beroende av i sitt vardagliga liv, till exempel kontakt med myndigheter och banktjänster över Internet. Tilliten är ett nödvändigt rekvisit för att medborgarna skall ändra sitt beteende och i allt högre utsträckning använda sig av IT. Tillit används här som ett övergripande begrepp omfattandes tillgänglighet, tillförlitlighet och integritet. Tillit är en subjektiv upplevelse och kan inte med nödvändighet hänföras till graden av teknisk säkerhet i ett system. För att IT skall användas för att inhämta och hantera information måste graden av tillgänglighet vara tillräckligt hög. En alltför hög tröskel för användande leder till att traditionella sätt att utföra ärenden söks. Komplicerade säkerhetslösningar kan göra användandet av

tjänster svårt eller långsamt, eller kan leda till opraktiska sökvägar för information.

Medborgarna har förutom rättigheter och behov också en del i samhällets säkerhetssträvanden. Alla användare av IT bör själva i så hög grad som möjligt följa de säkerhetsföreskrifter som finns och vidta de åtgärder som rekommenderas för ökad informationssäkerhet. Detta ansvar rör till exempel att uppdatera antivirusprogram med rekommenderade intervall och att upprätthålla en relevant kompetensnivå i förhållande till de aktiviteter man avser genomföra.

Inom näringslivet är behovet av säker kommunikation och informationsöverföring stort, även om behoven varierar beroende på verksamhetens natur. Utöver företagens eget behov av informationssäkerhet är deras roll i samhällets totala informationssäkerhet nödvändig att förhålla sig till. Det åvilar företagen ett stort ansvar som drivkraft bakom utvecklingen av såväl IT som säkerhetslösningar och som producent av allmänt tillgänglig teknik och tjänster samt som användare av IT att bidra till att öka informationssäkerheten i samhället och därmed ökat användande.

För att skydda den egna verksamheten är företagen själva ansvariga att vidta tillgängliga säkerhetsåtgärder. Det faktum att samhällsviktig infrastruktur och funktioner som den egna verksamheten är beroende av ofta finns utanför måste tas med i analysen av hela säkerhetsbilden. Säkerheten är då inte enbart en angelägenhet för den verksamhetsansvarige. Företag med samhällsviktig verksamhet har ett behov av att dels definiera vad som är att betrakta som samhällsviktigt och dels av att få tydliga direktiv om vad detta innebär för verksamheten och vilka särskilda åtgärder som är nödvändiga.

Statens behov av informationssäkerhet är tudelat. Dels är staten beroende av säker informationshantering inom den egna förvaltningen och dels i kontakten med övriga samhället. Projekt för att underlätta kontakten mellan stat och medborgare, till exempel 24-timmarsmyndigheter kräver en hög grad av informationssäkerhet.

Det finns även en internationell aspekt av statens behov av informationssäkerhet. För att Sverige skall kunna hävda sig i såväl internationella sammanhang som EU, måste informationssäkerhetsarbetet harmonieras med den internationella utvecklingen såväl gällande grad av informationssäkerhet som av säkerhetslösningar.

De behov som finns inom statlig sektor sammanfaller till stor del med det som finns i kommuner och landsting. Informationssäkerhetsfrågor bör ingå som en integrerad del i de risk- och sårbarhets-

analyser som tas fram för kommunerna. Det gäller såväl verksamhetsrelaterade som eventuellt integrerade risker. På kommun- och landstingsnivå finns det behov av ett förebyggande arbete för att säkerställa och förbättra de nationella försörjningssystemen, till exempel Stomnät för el och IT samt på såväl nätägar- som operatörsnivå. Informationssäkerhetsproblem skulle kunna lösas genom att man på central nivå utvecklade decentraliserade modeller. Inom landstingen är frågan om hanteringen av medicinska register angelägen att diskutera ur ett informationssäkerhetsperspektiv.

För aktörer vars uppgift till exempel är att förmedla elektroniska tjänster åt andra är situationen delvis en annan. Den verksamhetsansvariges möjligheter att påverka informationssäkerheten i system, som ligger utanför det egna området, är begränsade. Detta gäller framför allt kommunikationstjänster. Outsourcing - att lägga ut IT-system på driftsentreprenad, vilket innebär att en del av det dagliga ansvaret för driften av system flyttas till en extern part - blir allt vanligare. För mindre företag och kommuner innebär det en stor resursmässig och ekonomisk lättnad att kunna anlita andra aktörer med specialkompetens för delar av informationshanteringen, när denna inte är del av kärnverksamheten. Detta kan i många fall leda till förbättrad säkerhet. Det är dock ett inte försumbart problem att man genom att lägga ut informationshantering på entreprenad riskerar att få försämrad inblick i sin säkerhet och mindre möjlighet att påverka den. På motsvarande sätt är de flesta aktörer indirekt beroende av leverantörer av tjänster motsvarande till exempel elförsörjning eller transporter och därmed av informationssäkerhet i dessa system. Även i detta fall lämnas således en stor del av informationssäkerhetsproblemen till marknaden att lösa. Inom dessa områden kan det finnas behov av att kunna garantera tredje man viss informationssäkerhet, eftersom utbudet och valfriheten kan vara begränsat. Frågan om kommunikationstjänsterna är så viktiga att det kan vara motiverat att rikta särskilda krav.

Utgångspunkten för samtliga aktörskategorier är att varje verksamhetsansvarig genom ansvarsprincipen måste svara för sin egen informationssäkerhet, på samma sätt som för sin säkerhet i övrigt. Staten har i praktiken vare sig möjlighet eller anledning att i särskild ordning reglera vilken nivå för informationssäkerhet som bör finnas i respektive verksamhet. Undantaget är intresse i och ansvar för statens egen verksamhet. I den mån verksamheten omfattas av annan lagstiftning eller motsvarande måste informationssäkerhet kunna inrymmas utan närmare specificering. Utredningen konstaterar

dock att vissa legaldefinitioner, till exempel gällande elektroniska urkunder och inom e-handelsområdet, är nödvändiga eftersom tekniken är ny, vilket i viss utsträckning påverkar befintliga lagars tillämpning. Inom justitiedepartementet bereds för närvarande kommittédirektiv till en utredning om en översyn av vissa bestämmelser i 14 och 15 kap. brottsbalken ur ett IT-perspektiv. En fråga för översynen är i vad mån en elektronisk handling kan anses utgöra en urkund. Det finns dessutom ett behov av att utöka IT-relaterad kriminalteknisk verksamhet inom rättsväsendet. Med detta resonemang lämnas således en stor del av informationssäkerhetsproblemen till marknaden att lösa.

För att uppnå god informationssäkerhet måste medvetenheten om säkerhetsriskerna höjas. Utredningen konstaterade i sitt andra delbetänkande att informationssäkerhetsfrågorna kräver ökad eller riktad kompetens på alla nivåer i samhället. Medvetenheten är viktig på en organisations samtliga nivåer - från informationshantering till ledning. För att uppnå så god säkerhet som möjligt, är det viktigt att ledningens övergripande plan efterlevs av dem som hanterar information. På motsvarande sätt är det inte möjligt att uppnå fullgod säkerhet om de behov av säkerhet som de som hanterar informationen har, inte återspeglas av ledningen. Det finns därför ett behov av kompetenshöjande åtgärder som har större räckvidd än enbart till dem som mest frekvent hanterar informationen.

Höjd kompetens, och därmed medvetenhet, kan bidra till insikten att informationssäkerhetsriskerna inte är organisationsspecifika. I sitt andra delbetänkande konstaterade utredningen att integrationen av system i olika verksamheter ökar. Leverantörer och beställare är på grund av användningen av IT sammankopplade med distributören. Sammankoppling, via till exempel Internet, skapar risken att även obehöriga når information. Den egna organisationens säkerhet påverkas sålunda i stor utsträckning av säkerheten i kommunikationen med andra aktörer. De externa säkerhetsrisker som finns, till del på grund av andra aktörers bristande säkerhetsrutiner och osäkra överföringskanaler för information, kan påverka den egna organisationen. Av den anledningen bör säkerhetsstrategier omfatta såväl egen hantering och lagring av information, som överföring och mottagande av information.

Den större delen av informationssäkerhetsproblemen faller, som argumenterat ovan, inom respektive verksamhetsansvariges ansvarsområde. I de flesta fall är detta inte en uppgift för staten. Staten har dock ett ansvar att tillse att säkerheten håller en viss nivå i de

verksamheter som är att betrakta som *samhällsviktiga*. Det är också ett statligt ansvar att informationssäkerheten är tillräckligt hög inom de verksamheter som stödjer de primärt samhällsviktiga verksamheterna. Denna typ av verksamhet kan röra de mest intuitiva komponenterna av statens funktion för samhället, såsom att värna om rikets säkerhet, självbestämmanderätt etc. men även handla om fungerande el- och telenät och motsvarande funktioner som samhället har kommit att i hög grad vara beroende av. Om särskild personkontroll skall genomföras vid hantering av samhällsviktig verksamhet måste detta lagregleras. Frågan behöver därför beredas vidare.

3.2 Behov, möjligheter och problem ur säkerhets- och hotbildssynvinkel

Utredningen anslöt sig i sitt andra delbetänkande till den beskrivning av hotbilden som regeringen angav i propositionen prop. 2001/02:158 Samhällets säkerhet och beredskap. I generella ordalag är den hotbilden alltjämt giltig. Utredningen noterar dock att utvecklingen av tekniken går snabbare än utvecklingen av säkerhetslösningar, även om säkerhetsmedvetandet hos både leverantörer och kunder har ökat. Hotbilden är dessutom, på mer detaljerad nivå, föränderlig. Detta utgör i sig en utmaning då säkerheten inte kan lösas permanent utan måste utvecklas i en kontinuerlig process.

Den IT-relaterade hotbilden är mycket bred. Den spänner från vardagliga tekniska och handhavanderelaterade fel till potentiella terroristattacker. Det finns i debatten en tydlig fokusering på externa, allvarliga hot. Omfattande datavirusangrepp har drabbat Sverige – i likhet med många andra länder – vilket har medfört stora ekonomiska förluster för framförallt företag. Angrepp kan också vara riktade mot en specifik aktör. En strategi för informationssäkerhet måste uppmärksamma de antagonistiska hoten. Hot som kan härledas till tekniska brister eller felaktigt handhavande, vilka utgör den större delen av incidenter, är också synnerligen viktiga att hantera. Det kan vara svårt för en enskild aktör att, utifrån den egna verksamheten, se sin specifika sårbarhet i förhållande till en mer övergripande nationell hotbild. Det faktum att många små – till synes orelaterade – angrepp kan vara delar av en mer omfattande attack, pekar på vikten av en övergripande, ständigt uppdaterad hotbildsbeskrivning.

En samlad bild av sårbarheter och hot bör ligga till grund för respektive verksamhetsansvariges planering och säkerhetsåtgärder. Staten kan utifrån en bedömning av hot och sårbarheter dimensionera sina grundkrav för informationssäkerhet. De informationssäkerhetsåtgärder som görs i samhället bör vara en konsekvens av samma bedömning av verkligheten, vilket ställer stora krav på aktualitet då bilden snabbt kan förändras. Hotbilden måste för att vara tillförlitlig grundas på en utvecklad omvärldsbevakning. Genom denna kan svaga länkar identifieras och ansvaret för informationssäkerhetshöjande åtgärder fördelas bland relevanta aktörer.

Inom såväl offentlig som privat sektor finns verksamhet som är särskilt angelägen att skydda ur ett nationellt säkerhetsperspektiv. Det kan röra sig om verksamhet direkt kopplad till nationell säkerhet, som har säkerhet som sin utgångspunkt. För verksamheter som hanterar mycket känslig information, till exempel underlag för omvärldsanalys och hotbildsbeskrivning, är informationssäkerheten central.

Staten har för sådana verksamheter ett ansvar dels att tillse att kompetensförsörjningen är adekvat samt för andra åtgärder i den utsträckning som verksamheten är kopplad till nationell säkerhet eller till andra av statens ansvarsområden. Detta gäller i synnerhet sådan verksamhet som syftar till att förebygga allvarlig störning samt hantering i det fall störning ändå uppstår. Skydd av känslig information av annan karaktär, faller normalt inom företags eller organisations eget verksamhetsansvar.

3.3 Behov av helhetssyn

I proposition 2001/02:158 Samhällets säkerhet och beredskap anger regeringen att målet med informationssäkerhet bör vara att upprätthålla en hög informationssäkerhet i hela samhället. Ansvarsprincipen, likhetsprincipen och närhetsprincipen skall gälla, vilket innebär att den som ansvarar för informationsbehandlingssystem också skall ansvara för att systemet fungerar på ett riktigt sätt. För att undvika dubbelarbete och tillse att informationssäkerhetsarbetet blir heltäckande måste ansvaret för helhetsbilden åvila någon enskild aktör. Staten är härvidlag den enda möjliga aktören, dels på grund av kontinuitetsskäl och dels genom de åtaganden som staten har. Staten bör se till hela samhällets behov av informationssäkerhet

och vidta de åtgärder som rimligen inte kan åvila den enskilde systemägaren.

Utredningen redovisade i sitt andra delbetänkande de huvudsakliga funktioner och kontinuerliga arbetsuppgifter för offentliga organ som, utöver det ansvar som följer av ansvarsprincipen och oberoende av dagens organisationsstruktur och funktioner, nu kan identifieras inom informationssäkerhetsområdet. För att skapa en struktur för ett långsiktigt informationssäkerhetsarbete finns det ett behov av att överväga och fördela ett antal centrala uppgifter. Här kan till exempel nämnas tydliggörandet av nationell strategi, att föreslå och förmedla grundläggande regelverk, att ge råd och information till allmänheten och stöd till myndigheter, särskilda råd och stöd till samhällsviktiga myndigheter eller avseende viktiga system samt att förebygga, upptäcka, utreda och lagföra brottslighet som berör informationssäkerhet.

Aktörer som har ett särskilt stort behov av dessa åtgärder är stora användare av IT-system och ansvariga för särskilt viktiga system, till exempel statlig förvaltning, kommuner och landsting, näringsliv och allmänheten. De ansvariga statliga myndigheterna har olika roller, däribland tillsynsansvar, främjande, producent och konsument. Det statliga ansvaret kan utövas på olika sätt. Det kan omfatta regelstyrning, tillsyn, budgetstyrning eller myndighetsstyrning. Åtgärderna kan bidra till att öka tilliten till nya, IT-baserade funktioner vilket ligger i linje med regeringens IT-politiska ambition från år 2000, att Sverige skall vara världsledande i användningen av informationsteknik (IT).

Säkerhetsarbete kan vara en primäruppgift, en utpekad funktion eller ett krav. Informationssäkerhet skulle kunna jämföras med till exempel arbetarskydd, tekniska krav på elsäkerhet eller funktionella krav inom säkerhetsskyddet. Vissa av dessa krav med anknytning till informationssäkerhet finns reglerade i författningar med krav på sekretess, säkerhetsskydd och integritet.

Det är viktigt att beakta de delvis nya förutsättningarna för tillämpning av befintlig lagstiftning som uppstår vid ökad användning av digitala verktyg för att skapa och hantera information. En ökad användning av IT är påvisbar på alla nivåer i samhället och sannolikt inser inte samtliga berörda aktörer alla aspekter av skillnaden mellan pappersbaserad och elektroniskt lagrad information. Denna skillnad avspeglas inte heller i befintlig lagstiftning. Lagföring grundas på värdering av information och avgörandet av tvister är beroende av informationens ursprung och riktighet. Med

digital hantering av information följer att vi i dag ofta inte till fullo kan garantera vare sig informationens ursprung eller riktighet. För att man enligt juridiska principer skall kunna hantera digitalt genererad och lagrad information krävs därför åtgärder för att komma till rätta med de brister som finns.

Den svaghet det innebär att ett enskilt företag inte har tillräckliga motiv att se till en viss marknad i sin helhet utan enbart sin egen verksamhet, riskerar att på sikt påverka alla aktörer inom en given sektor. Gemensamma problem får sålunda individuella, och kanske inte alltid kompatibla, lösningar. En eventuell och allvarlig konsekvens av en sådan obalans mellan enskilda företag och marknad, är att samhällets behov av en tjänst eller vara inte tillgodoses. Staten kan vara den som tar ansvar för helhetsperspektivet genom reglering och styrning.

Informationssäkerhetsproblemen i samhället har dock visat att det finns ett behov av styrning inom området. Den offentliga sektorn har ett särskilt ansvar för att hantera de nya säkerhetsproblem som uppstår vid ökat användande av IT och som enskilda aktörer inte själva kan förväntas lösa. Staten måste upprätthålla tillräcklig förmåga att hantera oförutsedda eller nya typer av allvarliga störningar och kriser. Förmåga kan här anta flera olika skepnader för att utnyttjas i olika skeden av en störning, för att förebygga allvarliga störningar är kompetensuppbyggnad och kompetensförsörjning centralt. Utöver den proaktiva aspekten är det önskvärt att det finns en operativ förmåga som kan träda in under pågående störning för att övervaka, identifiera, stävja och återhämta.

Det är inte möjligt att dra en skarp gräns mellan vad som å ena sidan är problem som verksamhetsansvarig på företag eller myndighet själv har att lösa och å andra sidan störningar som är av sådan dignitet eller omfattning att det finns anledning för statligt ingripande. Virusangrepp som för ett företag innebär arbete och ökade omkostnader, kan på aggregerad nivå vara del av en störning som är att betrakta som ett hot mot landet. På grund av osäkerheten i bedömningen av en störnings dignitet är det rationella agerandet för staten att avvakta med avsteg från den verksamhetsansvariges ansvar. Osäkerheten i bedömningen har även sin grund i att nya typer av störningar kan bidra till situationer, som enskilda verksamhetsansvariga inte kan förväntas hantera på egen hand. Ett exempel är phishing (nätfiske), som av vissa befaras vara ett problem som kommer att öka i omfattning. Ett statligt agerande kan innebära att lyfta fram och informera om nya typer av hot och på så

sätt hjälpa företag och organisationer att arbeta förebyggande med säkerheten. Merparten av de angrepp som vi ser i dag är dock just störmoment och det är i enlighet med resonemanget ovan inte heller med nödvändighet så att en definierad åtskillnad på förhand behöver göras. Staten måste dock ha en beredskap för att kunna hantera störningar som kan nå en sådan omfattning att de är att betrakta som ett hot mot den nationella säkerheten.

3.4 Behov, möjligheter och problem för informationssäkerhetspolitiken

Mot bakgrund av utredningens resonemang om det offentliga åtagandet och informationssäkerhetsarbetets förutsättningar finns det enligt utredningen skäl att införa begreppet *informationssäkerhetspolitik*. Syftet är att föra samman informationssäkerhetsfrågorna som finns horisontellt, det vill säga gemensamma eller liknande informationssäkerhetsproblem, och vertikalt, det vill säga informationssäkerhet i verksamheten. Redan i dag är många av dessa föremål för regeringens politik, och enligt utredningen kommer det att bli nödvändigt med ytterligare samlande åtgärder.

Målet med den svenska IT-politiken är att Sverige skall bli ett informationssamhälle för alla (prop. 1999/2000:86). En förutsättning för att detta skall lyckas är att informationssäkerheten håller en sådan nivå att utvecklingen inte hämmas utan snarare stödjer en ökad användning av IT i fler verksamheter.

Inom ramen för en informationssäkerhetspolitik finns det ett behov av att samordna agerandet mellan Regeringskansliet och ansvariga myndigheter. Till utredningen har detta lyfts fram särskilt ur ett internationellt, men också ur ett nationellt perspektiv. Det finns även ett behov av att det offentliga håller sig informerat om utvecklingen inom den privata sektorn som kan komma att påverka informationssäkerhetspolitiken. Samtidigt bör ett av syftena med en informationssäkerhetspolitik vara att tydliggöra politikens innehåll. En del frågor som i dag betecknas som informationssäkerhetsfrågor är kanske inte det vid en närmare granskning. Det finns i dag redan system för hur frågor och konflikter skall lösas. Det finns en risk att begreppet informationssäkerhetspolitik blir för stort och döljer verksamheter som faktiskt går att skilja åt och på så sätt är lättare att hantera.

Många av frågorna inom informationssäkerhet är internationella. Det är ett relativt nytt område vilket gör att det finns möjligheter att vara med och påverka utvecklingen. För att lyckas med detta ställs det stora krav på god samordning och förmåga till samverkan, inklusive kontaktytor mellan myndigheter och den privata sektorn.

Den ökade användningen och det ökade beroendet av IT har lett till nya sårbarheter som måste hanteras, dels för att möjliggöra en gynnsam utveckling och dels för att förhindra allvarliga störningar – i vissa fall hot mot Sverige. Det är därför nödvändigt att finna åtgärder som kan leda till ökad säkerhet i informationssystem och därmed samhällets ökade säkerhet. Frågan om informationssäkerhet har ingen objektiv lösning. Det finns olika typer av aktörer som har skiftande säkerhetsproblem och säkerhetsbehov. Dessutom är hotbilden och framför allt aktuella sårbarheter föränderliga.

De sårbarheter som kopplas till IT är av olika slag och bör följaktligen hanteras på olika sätt. Därför är det viktigt att föra ett resonemang om den utgångspunkt hotbilden har. Det är inte utredningens avsikt att här beskriva kända sårbarheter och eventuella hot. Syftet är istället att föra ett resonemang om de bakomliggande frågeställningarna. En grov indelning kan vara funktions- eller verksamhetsberoende sårbarheter respektive aktörsberoende eller antagonistiska hot. Den förstnämnda kategorin omfattar tekniska fel och administrativa brister och den andra fysiska eller tekniska hot samt intrång och spionage.

För regeringens politik inom informationssäkerhetsområdet finns behov av principer som kan ligga till grund för överenskommelser och beslut om ansvarsfördelning och åtgärder. Den första principen skulle kunna handla om hotets ursprung och den andra om hotets möjliga konsekvenser. Sett ur statens synvinkel kan många administrativa och tekniska brister falla inom respektive verksamhetsansvarigs ansvar medan aktörsberoende och antagonistiska hot mycket snabbt kan bli statens ansvar att hantera särskilt när det gäller samhällsviktig verksamhet.

Den andra principen innebär att sannolikheten för statligt agerande ökar i takt med den potentiella allvarlighetsgraden. Ju svårare konsekvenser ett hot eller en brist kan få, desto sannolikare blir det att hanteringen måste involvera staten i någon form, till exempel brottsbekämpning, kontraterrorism eller totalförsvar.

Ansvar för förebyggande och hantering av funktions- eller verksamhetsberoende sårbarheter ligger huvudsakligen hos den verksamhetsansvarige och de som den ansvarige anlitar. Eventuella konse-

kvenser drabbar i första hand den egna verksamheten. Tekniska och ekonomiska effekter ligger också primärt inom respektive ansvarsområde, även om effekter för tredje part kan uppstå.

Ofta kan det vara svårt att urskilja informationssäkerhetsproblemen ur verksamheten, vilket gör det svårt att bedöma insatserna som behövs på politisk nivå. Flera områden är i dag reglerade (eller föremål för statliga åtgärder) ur en annan aspekt, men har explicita eller implicita krav på informationssäkerhet

Frågan om aktörsberoende eller antagonistiska hot är mer komplex. Föremål för aktioner kan visserligen vara en enskild verksamhetsansvarig, medan händelseförlopp och följder också kan involvera statens ansvarsområde i form av till exempel brottsbekämpning, olika brottsförebyggande åtgärder etc. Ytterst handlar det om ett led i försvaret av rikets säkerhet, vilket i synnerhet gäller samhällsviktig verksamhet.

Det ligger i statens ansvar för rikets säkerhet att förhindra och hantera IT-relaterade hot mot nationen. En möjlig väg att hantera detta är att skapa förutsättningar för att förebygga allvarliga incidenter och att förbereda för det fall att de ändå inträffar. Därför kan det vara motiverat för staten att inom ramen för en informationssäkerhetspolitik skapa möjligheter att förebygga och hantera sådana incidenter. För att staten skall kunna skapa förutsättningar för att förebygga allvarliga incidenter är det viktigt att öka medvetenheten om sårbarheter och hot i hela samhället. Medvetenhet, och i förlängningen en bredare säkerhetskompetens hos individer som i olika befattningar eller som privatpersoner hanterar IT, är nödvändigt för att staten skall kunna uppfylla sitt åtagande i det här avseendet. Ökad medvetenhet och större kompetens kan uppnås genom utbildningssatsningar på olika nivåer, till exempel att säkerhetsfrågor ingår i utbildningen och användningen av IT på grundskolenivå och mer specialiserade utbildningar som komplement till befintliga yrkesutbildningar. Staten har ansvar för helhetsbilden och med det följer ansvaret för att löpande ta fram korrekta analyser av säkerhetsläget i Sverige och i vår omvärld.

För att kunna förebygga och förbereda för informationssäkerhetsproblem i samhället krävs ett *långsiktigt arbete*. Det långa perspektivet måste bland annat ta hänsyn till teknisk utveckling, nya mönster i användningen av IT eller politiska förutsättningar i vår omvärld. En svensk strategi för informationssäkerhet måste formuleras med långsiktiga värden och måste samtidigt vara flexibel för att kunna möta förändringar. En strategi för informationssäkerhet

och lagstiftning på samma område måste med nödvändighet vara tekniskt kopplad, men vad som här avses är att en strategi inte kan tillåtas bli obsolet vid utvecklandet av ny teknik. Det innebär att strategin riktar in sig på tekniska företeelser men att den inte är beroende av att en specifik teknik används.

De övergripande, långsiktiga målen är nödvändiga riktmärken men det finns även ett behov av *beslutskraft i kort perspektiv*. De steg som skall tas mot informationssäkerhet måste specificeras med tidsangivelser. Detta blir än viktigare av det faktum att många olika aktörer, även i fortsättningen, kommer att ansvara för olika delar av informationssäkerhetsproblematiken.

För att kunna hantera incidenter som ändå inträffar är det nödvändigt med en *förmåga i realtid*. Det måste finnas ett väl fungerande system för krishantering inom detta område, som enligt tydliga riktlinjer snabbt träder i kraft vid en allvarlig incident. Det gäller även att kunna hantera de praktiska problem som följer på problem i IT-system.

Med dessa tre tidshorisonter bör det vara möjligt att skapa mål, styra och följa upp en informationssäkerhetspolitik.

3.5 Utredningens slutsatser av behovsbilden

Den IT-relaterade utvecklingen, som innebär ett ökat beroende av tekniken för hantering av information och en ökad interdependens mellan olika system och verksamheter, leder till en rad nya behov. Detta gäller såväl statliga och privata aktörer som medborgarna. Ett sätt att analysera behoven är att betrakta dem ur verksamhets- eller/och säkerhetssynpunkt. En på alla samhällsnivåer ökad medvetenhet om de säkerhetsrisker som kan förknippas med IT och generellt ökad kompetens är av synnerlig vikt.

Författningar som rör området informationssäkerhet måste kunna hantera att information finns i annan form än fysisk. Författningsändringar kan därför vara nödvändiga för att befintlig lagstiftning skall kunna tillämpas utan särskild specificering. Utredningen ser därför positivt på utredningen om brottsbalkens 14 och 15 kap. vars direktiv för närvarande bereds på justitiedepartementet. Det finns dessutom ett behov av att utöka IT-relaterad kriminalteknisk verksamhet inom rättsväsendet.

En viktig utgångspunkt för utredningen är att säkerhetsproblemen inte kan lösas definitivt utan måste hanteras i en kontinuerlig process. Däremot finns det ett stort behov av att samordna infor-

mationssäkerhetsarbetet. En samlad bedömning av hotbild, risker och sårbarheter bör ligga till grund för verksamhetsansvarigas planering och arbete.

Den verksamhetsansvarige har genom ansvarsprincipen ansvar för informationssäkerheten på samma sätt som för säkerheten i övrigt. De nya behoven är inte att betrakta som statliga per automatik. När det gäller samhällsviktig verksamhet är det dock rimligt att anta att staten har ett ansvar för att verksamheten skall uppfylla vissa krav. Detta gäller oavsett om denna drivs i privat eller offentlig sektor. Inom såväl privat som offentlig sektor finns det verksamheter som det är särskilt angeläget att skydda ur ett nationellt säkerhetsperspektiv. Det kan gälla sådana som har direkt koppling till nationell säkerhet eller verksamheter som hanterar stora mängder information som underlag till omvärldsbevakning eller hotbildsanalys.

Gränsen för vad som är verksamhetsansvariges ansvar och sådana situationer som motiverar ingripande från staten kan inte dras med säkerhet. Staten är den aktör som bör ha det övergripande ansvaret för helhetsbilden. Staten bör dessutom upprätthålla tillräcklig förmåga att hantera oförutsedda eller nya typer av allvarliga störningar och kriser. Det finns enligt utredningen skäl att införa informationssäkerhetspolitik som begrepp för att sammanföra de horisontella aspekterna (gemensamma eller liknande informationssäkerhetsproblem) av informationssäkerhet med de vertikala (informationssäkerhet i verksamheten).

Det finns ett behov av att samordna informationssäkerhetsarbetet mellan Regeringskansliet och ansvariga myndigheter och att fördela viktiga arbetsuppgifter. Samordningsbehov behövs såväl för det nationella arbetet som det internationella där Sverige har förutsättningar att vara med och påverka. Ett krav för att Sveriges genomslagskraft fortsatt skall vara stor i internationella fora är god samordning inom såväl offentlig sektor som mellan offentlig och privat sektor.

Ett annat syfte med informationssäkerhetspolitik bör vara att staka ut de övergripande målsättningarna för politiken. Detta torde bidra till en bättre förståelse för vad informationssäkerhet innebär.

Det finns ett stort behov av principer för ansvarsfördelning och åtgärder. En viktig fråga är vad som motiverar statligt agerande. En sådan princip skulle kunna ta sin utgångspunkt i hotets ursprung. Sannolikheten för att det skall finnas skäl för staten att agera ökar i takt med hotets allvarlighetsgrad. Motsvarande förhållande gäller för storleken på konsekvenserna.

4 Behov av strategi och konkreta åtgärder

Som utredningen pekat på i tidigare avsnitt är informationssäkerhet en frågeställning som har stor bredd och komplexitet och som måste involvera alla aktörer i samhället såväl privata som offentliga. Ett framgångsrikt säkerhetsarbete bygger i hög grad på hur pass väl olika grupper i samhället tar till sig problembilden, vilka åtaganden som respektive aktör är beredd att göra samt hur väl en samverkan inom och mellan dessa grupper av aktörer kan utvecklas. Informationssäkerhet handlar, enligt utredningens mening, i hög grad om hur samhället kan tillgodogöra sig den kapacitet som redan finns gripbar i form av människor, kompetens eller investeringar och är således inte bara en teknisk fråga eller ens enbart en fråga om ny informationsteknik och dess möjligheter.

I utredarens uppdrag ingår att utarbeta förslag till hur den svenska informationssäkerheten kan förbättras. I denna uppgift ingår därför att överväga vad den enskilda medborgaren kan göra, vad som bör falla på enskilda företag och som kan lämnas till marknaden respektive vad som faller inom det offentliga åtagandet. I uppgiften har utredningen även tolkat in att överväga vilka administrativa respektive tekniska åtgärder som kan aktualiseras liksom vilka olika former av administrativa, ekonomiska och informativa styrmedel som bör användas i sammanhanget.

Det är med ett visst beklagande som utredningen tvingas konstatera att övervägandena i detta delbetänkande, trots motsatta ambitioner i sakfrågorna, volymmässigt får en slagsida mot överväganden som rör det offentliga agerandet, särskilt det statliga, och de tekniska aspekterna av informationssäkerhet. Detta har skapat ett visst dilemma för utredningen. De överväganden och förslag som utredningen redovisar i det följande måste därför läsas i ljuset av utredningens direktiv, som i flera fall är direkta beställningar som rör statens eget agerande och som därför nödvändiggör en fördjupning av resonemangen. Detta bör inte uppfattas som ett

utryck för var utredningen anser att tyngdpunkten i informationssäkerhetsarbetet bör ligga.

Mot denna bakgrund har utredningen övervägt vilka behov som kan finnas för en utveckling av regeringens strategi för informationssäkerhet samt vilka konkreta åtgärder som bör genomföras. En sådan strategi för informationssäkerhet ställer krav på långsiktighet, beslutskraft i ett kort perspektiv och en operativ förmåga i realtid. En ökad informationssäkerhet måste därför bygga på en nationell strategi som kan omfattas av flertalet aktörer och intressenter som alla arbetar efter tydliga, övergripande målsättningar. Utredningen föreslår att den nationella strategin utvecklas enligt följande:

4.1 Det långsiktiga perspektivet: Strategi

4.1.1 Inledning

I utredningens andra delbetänkande redovisades att en nationell informationssäkerhetsstrategi bör ha ett långsiktigt framåtblickande perspektiv. Strategin kan ligga till grund för åtgärder på två till tre års sikt, vilka kan förnyas utifrån ändrade omständigheter. Strategin vänder sig till myndigheter, näringsliv och organisationer, men även till enskilda användare, då de flesta i dag är anslutna till olika lokala, nationella eller internationella informationstjänster. I det följande redovisar utredningen några utgångspunkter som bör ligga till grund för det fortsatta arbetet.

Utredningen föreslog i sitt andra delbetänkande att en strategi för informationssäkerhet bör inriktas mot att kunna:

- ligga till grund för politiska beslut och prioriteringar inom informationssäkerhetsområdet och förbättra samordningen av samhällets informationssäkerhetsarbete
- bidra till att reducera sårbarheten och uppnå en acceptabel risknivå i samhällets olika informationssystem och kritiska infrastruktur
- öka och fördjupa tilliten till informationstekniken, ligga till grund för trygg elektronisk kommunikation i privat och offentlig sektor samt säkra pålitliga nättjänster från offentlig sektor.

De överordnade målen för informationssäkerheten sammanfattades i några punkter, utifrån ett verksamhetsorienterat perspektiv:

- *Infrastruktur*: Samhällets infrastruktur för informationstjänster skall vara robust och säker i förhållande till de funktioner den utför. Kritiska informationssystem skall vara så säkra att en skada inte får större verkningar än som kan anses acceptabelt.
- *Verksamhet*: Det skall byggas en säkerhetskultur runt användandet och utvecklingen av IT i Sverige och informationssäkerhet skall vara en central faktor vid användandet av IT.
- *Medborgare*: Sverige skall ha en allmänt tillgänglig samhällsinfrastruktur för elektroniska signaturer, autentisering av avsändare av elektronisk information samt säker överföring av känslig information.
- *Styrning*: Regelverk som berör informationssäkerhet skall tillhandahållas och vidareutvecklas på ett samordnat och för användarna enkelt och översiktligt sätt.
- *Utbildning*: Det skall finnas möjligheter till utbildning inom informationssäkerhetsområdet för alla målgrupper.
- *Agerande*: Den informationssäkerhet som byggs upp skall stödjas av möjligheter till ingripande vid hot, incidenter, angrepp eller brottslighet som rör IT (till exempel dataintrång).

Informationssäkerhetsproblematiken omfattar ett stort antal aktörer och intressen, bland annat de som har informationssäkerheten som affärsidé och de som har den som utpekat ansvar. Informationssäkerheten är inte ett problem som kan lösas en gång för alla. Den tekniska utvecklingen bidrar till detta på åtminstone två sätt. Det finns en stor potential i den tekniska utvecklingen. Ökad tillgänglighet till tekniken förändrar i grunden sättet att hantera uppgifter och bedriva verksamhet. Detta är till stor del en positiv aspekt av utvecklingen och kan innebära ökad kostnadseffektivitet och tidsbesparing men leder samtidigt till ständigt ändrade omständigheter för informationssäkerheten. Det är ett känt faktum att ökat beroende av IT leder till nya sårbarheter. Den tekniska utvecklingen fortskrider även på den antagonistiska sidan och nya datavirus och angreppssätt utvecklas i snabbare takt än skyddet mot dem. Av dessa anledningar måste arbetet med att öka informationssäkerheten i samhället ske i en kontinuerlig process enligt långsiktiga målsättningar. Arbetet måste med nödvändighet vara tekniskt kopplat. Dock bör ett oberoende i förhållande till specifik teknik eftersträvas, eftersom åtgärder annars riskerar att snabbt bli föråldrade.

Elektronisk kommunikation medför alltså både sårbarheter och ömsesidiga beroenden. Den egna säkerheten inom en organisation eller ett företag är avhängig av att man samtidigt har hög säkerhet i den elektroniska kommunikationen med externa aktörer. Med elektronisk kommunikation ökar beroendet av att motparten har tillbörlig säkerhet i sina interna system. Ökad informationssäkerhet kan oftast uppnås endast om säkerhetsmedvetandet höjs hos aktörer på samtliga nivåer i samhället och att insikten att inget system är starkare än sin svagaste länk sprids. Det finns ett behov av att stärka intresset för informationssäkerheten i samhället hos alla inblandade parter.

Staten kan genom en strategi stödja de drivkrafter som redan finns i samhället för att stärka informationssäkerheten. Endast staten kan ha ansvar för helhetsbilden och i det ansvaret ligger även att förmedla helhetsbilden samt att fastställa grundläggande krav och regler för informationssäkerhetsarbetet i samhället, såväl inom offentlig som privat sektor.

Enligt regeringens översiktliga strategi enligt proposition 2001/02:158 Samhällets säkerhet och beredskap skall störningar i samhällsviktig verksamhet kunna *förhindras* eller *hanteras*. Vidare bör underrättelse- och säkerhetstjänstens arbete *förstärkas*.

Utredningen anser att detta är en riktig utgångspunkt men att det finns motiv för en fördjupning och tillägg till det skrivna: störningar i samhällsviktig verksamhet bör kunna *förebyggas* och *förberedelse* för att minimera konsekvenserna bör bedrivas. Ett sådant tillägg lägger ytterligare fokus på det förebyggande arbetet. Att *förebygga* innebär ett proaktivt arbete för att, genom till exempel goda säkerhetsrutiner, såväl tekniska som administrativa, undvika allvarliga incidenter. I begreppet *förbereda* ligger beredskapen att hantera incidenter när de ändå inträffar. Förberedelserna bör vara av såväl teknisk som administrativ karaktär. Det är en i sammanhanget viktig insikt att någon absolut säkerhet, i bemärkelsen att incidenter garanterat helt kan undvikas, inte är möjlig att uppnå. Ett effektivt proaktivt arbete kan dock bidra till att avsevärt minska risken för och konsekvenserna av allvarliga incidenter. Det är nödvändigt att kunna hantera effekterna av en incident, likväl som att ha en god beredskap. För att förhindra allvarliga informationsattacker mot svenska intressen bör underrättelse- och säkerhetstjänsternas arbete förstärkas och informationen bearbetas, så att relevant information kan delges berörda. Möjligheten att *delge* informationen är här central. Detta innebär att även myndigheter

som i dag inte får del av underrättelser i framtiden bör kunna delges relevant information för att på ett mer effektivt sätt kunna förebygga och förhindra incidenter. Det är dock viktigt att påpeka att denna typ av information kan vara känslig. Det är därför nödvändigt att det utarbetas ett system för att avidentifiera information så att inte eventuella källor riskerar att röjas samt att tillse att information inte hamnar hos obehöriga.

Slutligen måste begreppet *hantera* omfatta den förmåga att agera och ingripa som skall finnas när brott begås. Det är därför viktigt för allmänhetens förtroende att Polisen har tillräckliga resurser och kompetens att ingripa och utreda brott inom informationssäkerhetsområdet. Även det författningsmässiga stödet behöver utvecklas. Inom EU pågår ett arbete som syftar till att bland annat kriminalisera vissa intrång i informationssystem, systemstörningar etc. Utredningen återkommer till den internationella dimensionen i kapitel 5.

4.1.2 Innehåll i en nationell strategi för informationssäkerhet

Utredningen anser att följande moment bör ingå i en nationell strategi för informationssäkerhet:

Internationell koppling

En grundläggande utgångspunkt i strategin bör vara att förhålla sig till Sveriges position i olika internationella sammanhang. Informationssäkerhet är en förutsättning för att Sverige skall kunna leva upp till målsättningen att vara ett informationssamhälle för alla. Sveriges position skall upprätthållas genom ett starkt internationellt engagemang och deltagande i tongivande forum inom EU, OECD och sektorsamarbeten. Bristande säkerhet i samhällsviktiga system kan få till följd att förtroendet för Sverige som ledande IT-nation minskar. Ett minskat förtroende kan i förlängningen bidra till att Sveriges genomslag i internationella fora försämras. Sverige har inom EU ett gott rykte beträffande informationssäkerhet. Det medför att vi också kan agera inom andra områden och få ett större genomslag för våra idéer och förslag.

Sveriges goda rykte inom informationssäkerhet har bland annat kommit till uttryck genom att Sverige blivit tillfrågat om att evaluera

olika säkerhetsprodukter för EU. En förutsättning för att Sverige ska bibehålla sitt goda anseende är att vi har en långsiktig strategi för vårt arbete. Det är också viktigt att Sverige har ett regelverk som förhåller sig till EU:s regelverk på ett sådant sätt att det är lätt att tillämpa och följa.

Förtroende

Nationellt är det viktigt att det skapas ett förtroende för den nya tekniken så att medborgarna känner att de kan använda den med bibehållen trygghet, säkerhet och integritet. Detta kan ske genom utbildning och informationsspridning. Syftet är att öka medvetandet om de risker, men också om de möjligheter till skydd, som finns. Skulle förtroende saknas eller vara bristfälligt kommer inte medborgare, näringsliv eller offentlig sektor att använda sig av informationssystem varvid tillväxten och utvecklingen riskerar att hämmas. En grundläggande förutsättning för förtroende är att det författningsmässiga skydd som finns i dag kan upprätthållas även när information hanteras i digital form. Den trygghet, säkerhet och integritet som lagstiftaren haft som utgångspunkt måste kunna garanteras.

Främjande av användning av IT

Sverige har som IT-politisk målsättning att vara ett informationssamhälle för alla. Under en rad av år har staten varit initiativtagare till en bred utbyggnad av infrastrukturen för att främja användandet av nya tekniska tjänster. Regionalpolitiska motiv och strävan efter tillväxt har drivit denna utveckling framåt. Sverige har haft ett framgångsrikt näringsliv inom IT-branschen vilket har bidragit till att vi är en ledande IT-nation. Det är nu viktigt att främja användningen av IT på bredden, vilket ökar förutsättningarna för tryggad sysselsättning och bibehållen välfärd. Dessa åtgärder är ett ansvar som den offentliga sektorn delar med näringslivet.

Samverkan

Sverige är inom informationssäkerhetsområdet en liten nation med begränsade resurser. Vi har inte råd att bygga parallella strukturer för att lösa gemensamma problem, då det skulle kunna leda till

resursbrist inom ett antal viktiga områden. Det är nödvändigt att näringsliv och offentlig sektor samverkar för att bäst utnyttja resurser. Den offentliga sektorn kommer att ha behov av att kunna utöva tillsyn, upprätthålla rättsstaten och att tillgodose sina egna behov som konsument av informationssäkerhet. Det kommer också att finnas åtskilliga områden där ett samutnyttjande av vissa kompetenser mellan näringslivet och offentliga sektorn är den mest rationella lösningen.

Kompetensutveckling

En orsak till att informationssäkerheten generellt sett inte ligger på en acceptabel nivå är att tillräcklig kunskap saknas om de risker och hot som förekommer. Detta är också ett problem när det gäller medborgarnas användning av olika IT-tjänster. Informationssäkerhet är i dag inget som automatiskt ingår när ett IT-system upphandlas eller när man köper en persondator. Ofta måste beställaren själv precisera vad som skall tillföras för att erhålla en acceptabel säkerhetsnivå. Här har hela samhället en uppgift att, genom att medvetandegöra och stimulera kompetensutveckling, visa på riskerna men också påvisa vilka möjligheter som finns att åtgärda problemen. Detta är av stor vikt inom verksamhet som kan betraktas som samhällsviktig. Även för den enskilda medborgaren är det viktigt att åtgärder vidtas. En vanlig hemdator utsätts för de risker som förekommer inom dagens IT-värld. När samma dator sedan används för att till exempel besöka en 24-timmarsmyndighet, kan den utgöra ett hot mot de större systemen.

Samhällsviktig verksamhet

En del av den samhällsviktiga verksamheten är den kritiska infrastrukturen. Trots att begreppet samhällsviktig verksamhet inte är klart definierat kan utredningen konstatera att just den kritiska infrastrukturen inom bland annat el, tele, betalningssystem och vattenförsörjning är samhällsviktiga verksamheter. Dessa system är så vitala för att samhället skall kunna fungera att det inte är acceptabelt att de skulle kunna slås ut av en IT-relaterad incident. Verksamhet som syftar till att skydda infrastrukturen benämns skydd av kritisk infrastruktur, CIP (Critical Infrastructure Protection).

Skyddet av de fysiska delarna av informationssystemen inom dessa infrastrukturer benämns skydd av kritisk informationsinfrastruktur, CIIP (Critical Information Infrastructure Protection). Med ett bredare uttryck kan detta kallas skydd av samhällsviktig verksamhet. Exempel på sådant är informationssystemen i elförsörjningen som styr hur elen distribueras i landet.

Det offentliga åtagandet

Statens roll är flerfaldig. Det åvilar staten att lösa uppgifterna att förebygga, förhindra och hantera IT-relaterade incidenter som är av sådan omfattning att det inte är rimligt att begära att drabbade själva skall vidta fullständiga åtgärder. För att det skall vara möjligt måste staten vara den som har det övergripande perspektivet och ansvar för att korrekt omvärldsbevakning kontinuerligt tas fram.

Staten måste också skapa ett organisatoriskt system för informationssäkerhetsarbetet som garanterar kontinuitet och kvalitet. Utredningen återkommer till detta i sitt slutbetänkande.

Uppgiftsområden för offentliga organ inom informationssäkerhet

En uppgift för offentliga organ bör vara att upptäcka och identifiera säkerhetsbrister i samhällsviktig verksamhet. Det kan ske genom sårbarhets- och riskanalyser för att upptäcka och identifiera förhållanden som kan utlösa allvarliga störningar. Informations-, utbildnings- och övningsinsatser som bygger på resultatet av sådana analyser är angelägna. Stor öppenhet bör tillämpas beträffande resultatet av sårbarhets- och riskanalyser för att öka medvetenheten om eventuella allvarliga brister och göra det möjligt att vidta säkerhetsförbättrande åtgärder. Underlag för sårbarhets- och riskanalyser måste dock kunna lämnas under sekretess.

Offentliga organ bör också kunna bedriva en säkerhetsinriktad revision i sin egen verksamhet. De bör dessutom verka för att en sådan revision i större utsträckning bedrivs inom den privata sektorns revision. De metoder som användes för att säkra informationssystemen inför millennieskiftet bör kunna användas i denna typ av revision. En framgångsrik säkerhetsrevision förutsätter att ledningsnivån, som är ytterst ansvarig, inom myndigheter, kommuner, landsting, näringsliv och organisationer aktivt engagerar sig i arbetet.

Att ha en god informationssäkerhet innebär att kunna lösa såväl vardagliga problem som att ha en beredskap för att hantera allvarliga, omfattande incidenter som möjligen även drabbar andra verksamheter än den egna. Ett företags egen, grundläggande vardagssäkerhet är ingen statlig eller offentlig angelägenhet. Att skydda de interna informationssystemen, såväl tekniskt som administrativt, och att ha en beredskap för att hantera incidenter är ett ansvar som åligger var och en som förvaltar ett system. Staten kan dock ha en roll i att stimulera till säkerhetsåtgärder och att öka medvetenheten om sårbarheten i informationstekniken.

Ett företag har sålunda ansvar för sina egna system och privatpersoner har ansvar för sina datorer. Det kan dock vara en svårighet för den enskilde att överblicka aktuella sårbarheter. För att skapa adekvata risk- och sårbarhetsanalyser krävs en noggrann omvärldsanalys och en överblick över hotbilden som sträcker sig längre än enskilda system och användare. Detta är inget statiskt dokument som användare kan ta del av utan en process som måste bedrivas med kontinuitet. Ansvaret för helhetsbilden över samhällets samlade IT-relaterade hotbild är en uppgift som bör åvila offentliga organ. Staten står för resurser och en kontinuitet, som inte kan vare sig krävas eller garanteras av någon annan aktör.

Signalskydd är ett viktigt medel för att åstadkomma bättre informationssäkerhet och bör vara en naturlig del av det offentliga åtagandet inom informationssäkerhetsarbetet. Signalskydd i Sverige har historiskt sett haft en stark koppling till totalförsvaret och behovet att skydda information har varit knutet till sekretesslagen (1980:100). Civila myndigheter med flera begär i allt större omfattning stöd med uppgifter rörande signalskydd även för hantering av skyddsvärd information som inte omfattas av sekretess.

Det är, som argumenteras ovan, rimligt att ansvaret för den dagliga säkerheten åvilar varje användare, förvaltare eller ägare av informationsteknik. För att hantera allvarligare incidenter, som kan komma att påverka den nationella säkerheten eller nationella intressen, måste dock staten ha ansvaret. Det handlar om att kunna skydda medborgarna mot övergrepp och oegentligheter samt att säkerställa att samhällsviktig verksamhet bedrivs med höga krav på funktionalitet och säkerhet. Det gäller även när nationella intressen bevakas inom EU och i internationella organ.

Staten måste också ha ansvar för spelreglerna inom informationssäkerhetsområdet. Mot bakgrund av sin överblick över samhällets säkerhetssituation och den hotbild som kan kopplas till informa-

tionssäkerheten bör staten skapa en struktur för att hantera extraordinära händelser.

Staten har också ett eget intresse för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sin roll som ansvarig för myndighetsutövning och som ägare.

4.2 Det kortsiktiga perspektivet

4.2.1 Inledning

För att uppnå de mål som stipuleras i den nationella strategin för informationssäkerhet behöver strategin kompletteras med förslag på åtgärder. De föreslagna åtgärderna är tänkta att dels uppmärksamma det kortsiktiga perspektivet och dels att rikta in arbetet mot strategins mer övergripande målsättningar.

Områden som bör bli föremål för åtgärder är bland annat organisation, ansvarsfördelning och befogenheter inom informationssäkerhetsområdet. Utredningen avser inte att föreslå några avsteg från ansvarsprincipen, närhetsprincipen och likhetsprincipen. Dessa är fundamentala och skall utgöra grunden för utformningen av åtgärdsförslag.

Utredningen konstaterar att det inte går att lösa informationssäkerhetsfrågan slutgiltigt utan att åtgärder även framöver kommer att vara nödvändiga inom detta område. Däremot finns det ett behov av en inriktning för de åtgärder som behöver vidtas. Utredningen har i avsnitt 6.2 och 6.3 föreslagit vilka åtgärder som behövs för att underlätta samverkan mellan offentlig och privat sektor, men också inom den offentliga sektorn.

Det är önskvärt att staten fastställer en uttalad politisk inriktning inom informationssäkerhetsområdet. En sådan åtgärd får till följd att Sverige på ett bättre sätt kan hävda sin position i internationella sammanhang. Ett sätt att uppnå en tydlig inriktning för arbetet är att göra informationssäkerhet till ett eget verksamhetsområde. På så vis skapas bättre förutsättningar för en god samordning mellan myndigheter och ett bättre resursutnyttjande. Med tydliga mål och utpekat ansvar minskar risken för dubbelarbete och kraftsplittring.

Sverige, tillsammans med resten av den del av världen som har stort beroende av IT-tjänster, står inför ett vägskäl när det gäller förtroendet för dessa IT-tjänster. Det är naturligt att riskerna med IT ökar med ökat beroende. I dag kan stora värden stå på spel. Det

är viktigt att bygga upp förtroendet för dagens teknik genom att visa på möjligheterna och satsa på säkerhetshöjande åtgärder.

Informationstekniken är inte geografiskt bunden och är på så sätt en global fråga. De åtgärder som erfordras för att skapa förtroende för den nya tekniken nationellt behöver samordnas med den internationella utvecklingen. Ett ökat samarbete mellan nationer kan också vara ett sätt att öka förtroendet för utvecklingen. Det är vikigt att Sverige utnyttjar sitt goda rykte inom området för att påverka andra nationer och att tillsammans med dem medverka till förändringar. Dessa förändringar kan röra multilaterala överenskommelser, harmonisering av lagstiftning mot IT-brott, åtgärder för att begränsa spridning av spam eller andra risker som den nya tekniken har medfört. En viktig fråga är möjligheten att identifiera och lagföra personer som utan att finnas i landet åstadkommer skada. I dag är det svårt att lagföra de som genomför attacker eller sprider skadlig programkod. Detta är ett problem som kan leda till bristande förtroende.

Nationellt behöver kunskapen om vad som kan göras för att skapa en högre informationssäkerhet öka. Sätt att bidra till en sådan utveckling är utbildning och målinriktade informationskampanjer mot olika intressegrupper. Det bör vara en målsättning att alla som använder en dator på något sätt också är medvetna om vilka risker som finns och vad som kan göras för att minska dessa risker. Denna uppgift delas av offentlig och privat sektor.

Det är viktigt att medvetande- och kompetenshöjande åtgärder kommer upp på dagordningen på alla ledningsnivåer. För att få chefer på alla nivåer att ta ansvar för informationssäkerheten krävs att de har kunskap om vad de är ansvariga för.

När det gäller samhällsviktiga system är det inte bara en fråga om förtroende utan också om trygghet och säkerhet i samhället samt den personliga integriteten. Skulle förtroendet för ett samhällsviktigt system svikta på grund av bristande informationssäkerhet, kan detta direkt få politiska konsekvenser. Det är därför ett ansvar för den offentliga sektorn att medverka till ökat förtroende för dessa system. Ytterst kan detta endast ske genom påvisat hög säkerhet.

Förtroende

Förtroendefrågan är således av grundläggande betydelse. Ett problem i sammanhanget är att en del organisationer tvekar inför att visa andra aktörer den öppenhet som krävs för att tillsammans lösa känsliga säkerhetsproblem. Det finns exempel på organisationer som tvekar att ge staten ett sådant förtroende. De flesta organisationer har hög sekretess kring sina IT-säkerhetsförhållanden. Organisationen kan dock tvingas välja mellan mindre effektiva åtgärder eller att exponera sina allra känsligaste informationssäkerhetsproblem. Problemet blir särskilt tydligt för de organisationer som själva saknar kompetens på området. Dessa saknar möjlighet att själva bedöma hur seriösa och kompetenta enskilda aktörer är. Statliga aktörer och sannolikt också vissa icke-statliga aktörer med ansvar för IT-system av samhällsviktig eller kritisk natur, måste kunna vända sig till någon som kan garantera sekretessen kring dessa system. Detta gäller i synnerhet system som är av betydelse för rikets säkerhet.

Användandet av IT är en viktig tillväxtfaktor. Ur ett demokratiperspektiv är det viktigt att utvecklingen inom IT-området sker i en för samhället positiv riktning. Genom projekt som 24-timmarsmyndigheter kan medborgare snabbt och enkelt erhålla information och få tjänster utförda. Myndigheternas servicenivå har på detta sätt ökat betydligt. Ett par av de mest påtagliga exemplen är att det numera är möjligt att deklarera samt att sköta sina bankaffärer via Internet. Dessa tjänster kommer inte att utnyttjas om kunderna saknar förtroende för säkerheten. Förutsättningen för en gynnsam utveckling är att informationssäkerheten utvecklas i samma takt som olika tjänster blir tillgängliga. Det är också viktigt att den information som delges via till exempel hemsidor är pålitlig. Riktigheten i de webbsidor som delger information inom ett samhällsviktigt område måste så långt det är möjligt kunna garanteras. Detta gäller till stor del även inom näringslivet. Om kunder eller andra som har en affärsrelation med ett företag inte har förtroende för hur informationssäkerheten hanteras tappar man också lätt förtroende i övrigt för det företaget.

Kompetens

Tillgången till kompetent personal inom informationssäkerhetsområdet påverkar hur väl vi kan hävda oss mot de risker som finns inom IT-området. I kapitel 8 redovisar utredningen mer utförligt viktiga frågor för kompetensförsörjningen. Det kommer att behövas ökad kompetens för att klara det som ligger inom statens ansvarsområde. Det är ett statligt åtagande att tillse att utbildningsinsatserna är tillräckliga. Det är däremot ett gemensamt intresse för näringslivet och den offentliga sektorn att sätta upp gemensamma krav på denna utbildning. Då informationssäkerhet är ett problem för hela samhället är det också viktigt att möjliggöra erfarenhetsutbyte mellan olika organisationer. Staten kan inte lösa sina problem på egen hand. Tillsammans kan privat och offentlig sektor dock uppnå bättre resultat än i dag. Vi måste hushålla med resurserna i form av kompetent personal.

Samverkan

Faktorer som kan försvåra samverkan bör minimeras. Staten får inte konkurrera med näringslivet på ett otillbörligt sätt. Det finns dock viss verksamhet inom det statliga ansvarsområdet, där endast staten kan agera. Det är därför viktigt att staten har kompetens för att kunna agera om något händer inom ett för samhället viktigt system eller ett system som har koppling till rikets säkerhet. Kompetensen måste höjas vad gäller tekniska principer för IT-säkerhet, både på ett allmänt plan och mer specifikt beträffande produkter på marknaden. De tekniska detaljkunskaperna om produkter, protokoll, kända tekniska säkerhetsbrister och virus m.m., måste också hela tiden uppdateras. Tillgång till kompetens får inte variera med konjunkturen, utan måste alltid säkerställas. För att veta hur samhället skall fördela sina resurser på ett effektivt sätt krävs det att begreppet samhällsviktiga system definieras.

Samhällsviktig verksamhet

Kriterier bör tas fram för identifiering av samhällsviktig verksamhet och system. Bedömningen av vad som är samhällsviktigt måste även omfatta systemets betydelse för andra funktioner. Vid en sådan analys kommer det att utkristalliseras en rad beroendeförhållanden

till andra system som därmed också kan komma att betraktas som samhällsviktiga. Av resultatet av en sådan analys bör det gå att dra slutsatser, dels om huruvida systemet är samhällsviktigt eller ej, och dels vilka beroenden som systemägaren själv kan ta ansvar för. Vissa beroenden kan man inte rimligen kräva att en enskild systemägare bör ta ansvar för. Som exempel kan nämnas att det inte ligger inom en systemägares ansvar att i en situation, där det råder brist på drivmedel i en region eller nationellt, se till att ett reservelverk får drivmedel. I dag saknas uttalade politiska mål för vilka krav som skall ställas på den kritiska infrastrukturen. Denna struktur är en del av de samhällsviktiga systemen. Prioriterade infrastrukturer, sett ur ett informationssäkerhetsperspektiv är el, tele samt vattenförsörjning. Även betalningssystemet som bygger på Internet är ett samhällsviktigt system. Inom dessa områden finns det ett stort ömsesidigt beroendeförhållande. Ägandebilden är både statlig, kommunal och privat. Detta gör att det krävs en väl fungerande samverkan för att informationssäkerheten skall ligga på en acceptabel nivå. Ett område som hittills inte har betraktats som prioriterat inom informationssäkerheten är etermedier (radio och tv), varken när det gäller produktion eller distribution. Radio och tv digitaliseras i alla led. Denna utveckling går fort och gör att kraven på informationssäkerhet ökar. Det bör övervägas om inte detta område också bör prioriteras. En erfarenhet från stormen i södra Sverige vintern 2005 är att radion hade en viktig roll i samhällsinformationen.

Helhetssyn

Utan helhetssyn på de tekniskt relaterade hoten kommer staten aldrig att kunna skydda det allmänna och enskilda från kvalificerade aktörers angrepp. Helhetssyn kräver tillgång till relevant information, såväl öppen som hemlig. Detta utgör ett problem eftersom den kritiska information som finns inom underrättelse- och säkerhetstjänsterna när det gäller IT-relaterade hot inte utan vidare kan göras offentlig.

Källor, metoder och viss information som följer med det internationella samarbete som dessa organisationer bedriver, måste skyddas. I vissa fall kan information erhållas under villkoret att den inte får lämnas vidare. I många fall går problemen att lösa genom att informationen anpassas till mottagarens behov eller genom att en indirekt kunskapsöverföring sker genom att personal från under-

rättelsetjänsterna använder den kunskap de erhållit vid olika former av stödverksamhet, till exempel den kontrollverksamhet som Säkerhetspolisen (Säpo) bedriver eller den aktiva IT-kontroll som Försvarets radioanstalt (FRA) genomför.

4.2.2 Ett gemensamt kommunikationsnät för samhällsviktig verksamhet

Enligt ansvarsprincipen ansvarar i dag varje enskild myndighet för sin egen Internetanslutning. Det innebär att det finns varierande lösningar ur både tekniska och administrativa perspektiv. Trots denna stora variation finns det ett antal komponenter och tjänster som återkommer hos det stora flertalet myndigheter. Detta gör att det går att tala om en typisk Internetanslutning.

En Internetanslutning är i ständigt behov av drifts- och underhållsåtgärder för att funktionen skall vara säkerställd. Myndighetens egen IT-organisation är oftast ansvarig för att detta hanteras och att uppdateringar och övervakning sker. Skall detta kunna skötas på ett tillräckligt säkert sätt krävs det i dag att det sker under dygnets alla timmar. En Internetanslutning är ständigt utsatt för försök till olika typer av angrepp i olika avseende. Övervakas anslutningen endast under ordinarie arbetstid, som i de flesta fall sker, kan en IT-incident inträffa utan att myndigheten blir medveten om detta innan det är för sent.

Ett mycket effektivt sätt för att förbättra informationssäkerheten när det gäller övervakning och underhåll av Internetanslutningar för samhällsviktig verksamhet skulle kunna var att bygga ett säkert nät för denna typ av verksamhet. Flertalet länder har denna typ av nätverk, det vill säga så kallat GOV NET. Hur detta skulle kunna realiseras utan att därför åsidosätta ansvarsprincipen eller den fria konkurrensen, liksom frågor om vilka som skulle delta och andra relevanta frågor bör utredas ytterligare.

4.2.3 Säkrare Internet

Samhället är i dag starkt beroende av Internet som kommunikationssystem för bland annat information, transaktioner, logistik, industriella processer, tillhandahållade av offentlig service samt för underhållning. Internet bygger på nätverkstekniken Internet Protocol (IP).

I kombination med domännamnssystemet (DNS) och det användarvänliga gränssnittet World Wide Web som använder presentationsprotokollet *Hyper Text Markup Language* (HTML) fick Internet sitt genombrott i början av 1990-talet.

Allt fler företag baserar sin verksamhet på Internet. Även samhällsservice från stat, landsting och kommuner sker alltmer via Internet, vilket ökar möjligheterna till tvåvägskommunikation och dialog mellan samhällets institutioner och medborgarna. Produktivitetsvinsterna av ett väl fungerande Internetsystem är mycket höga. Internet fungerar också som en snabb informationskälla vid kriser och allvarliga händelser. Användningsområdet vidgas hela tiden till exempel genom nytillkommande tjänster som telefoni, radio och TV.

Den snabba ökningen av Internetanvändare åtföljs dock av en växande sårbarhet i befintliga system. Antalet IT-incidenter har under en följd av år ökat. Funktionsstörningar eller antagonistiska angrepp kan få allvarliga konsekvenser. Som Post- och telestyrelsen (PTS) redovisat i ett förslag till strategi för att säkra Internets infrastruktur (PTS-ER-2005:7) har sårbarheten utnyttjats och exponerats vid bland annat överbelastnings- och intrångsattacker, fysiska avbrott och spridning av bland annat virus, trojaner och maskar[1]. Det är mycket angeläget att funktionsförmågan i Internet kan upprätthållas och därigenom också förtroendet för Internet som kommunikationssystem. PTS förslag har remissbehandlats och är för närvarande föremål för Näringsdepartementets vidare överväganden. PTS har i rapporten förklarat att myndigheten kommer att gå vidare med ett antal åtgärder för att förstärka infrastrukturen.

Virus, trojaner och maskar är exempel på skadlig kod som länge uppmärksammats. De hanteras normalt genom brandväggar och antivirusprogram som numera finns på marknaden med god kvalitet. De kräver säkerhetsmedvetande hos användaren, men är relativt enkla att installera och uppdatera. Det finns också program och tekniska system som på annat sätt än genom den direkta förstörelsen kan vara ett hot mot integritet eller bas för kapning av hela nätverk av datorer. Dessa så kallade spionprogram och deras funktioner kan ibland vara av relativt trivialt slag, avsedda att samla in information om vilka som besöker en viss webbsida. Men de kan också leda till

[1] **Virus** är skadlig kod som kopierar sig själv till filer på datorn, som på så vis blir allt mer smittad. **Trojan** är en annan typ av skadlig kod. Trojanen finns i ett program som i sig verkar ofarligt. **Mask** är ytterligare en typ av skadlig kod. Masken kopierar sig vidare mellan datorer (ofta med hjälp av e-post).

integritetskränkningar och vara ett hot mot allmänhetens förtroende för Internet. En del av dessa program kan även möjliggöra för antagonistiska hot att via fjärrstyrda datorer skapa plattformar för vidare angrepp som användaren är helt omedveten om.

Spam[2] används allt oftare för att sända så kallade spionprogram eller virus och utnyttjas även för bedrägerier. Ett relativt nytt hot är nätfiske (eng. phishing). Det är en metod som syftar till att samla in känslig information. De utges ofta komma från en seriös avsändare, men med falsk avsändaradress eller falsk webbsida som ger ett autentiskt intryck. Avsikten är att få mottagare att lämna ifrån sig personlig eller ekonomisk information, lösenord, personnummer, kontonummer etc. som sedan kan utnyttjas för bedrägerier.

Organisationers och företags domännamn är mycket viktiga. Det är därför angeläget att förtroendet för toppdomänen .se bibehålls och stärks då samhället strävar mot en mer digitaliserad offentlig sektor, e-handeln växer och internationell kommunikation ökar inom allt fler sektorer. Med en elektroniskt sammanhållen förvaltning i sikte får inte förtroendet för toppdomänen skadas.

I och med att ett nytt regelverk för toppdomänen infördes, ökade antalet domänansökningar kraftigt. Då ingen förprövning hittills skett för anskaffandet av domäner, vilket i sig har gynnat företag, organisationer och privatpersoner, har det visat sig finnas en risk för att oseriösa användare kan använda ortsnamn och namn som kan associera till kända företeelser, företag och organisationer för egna syften. Därmed kan förtroendet för toppdomänen komma att skadas och många känna osäkerhet inför att göra till exempel ekonomiska transaktioner eller ta del av patientjournaler från sjukvården över Internet. Det är angeläget att dessa frågor också beaktas vid etableringen av eu-toppdomänen.

Infrastrukturen för Internet, som består av såväl fysiska som logiska element måste skyddas för att möjliggöra ett säkrare Internet. Den utgör i dag en samhällsviktig verksamhet, även om Internet utgör en infrastruktur med viss tolerans mot störningar genom mångfalden av förbindelser och utformningen av IP-protokollet. Sårbarhet och brister i säkerheten kan följas och åtgärdas på flera sätt, bland annat vad gäller störningar i domännamnssystemet och skydd mot manipulerad information.

De leverantörer som svarar för driften av infrastrukturen och de operatörer som tillhandahåller tjänster på nätet har det främsta ansvaret

[2] **Spam** är e-postmeddelande, ofta reklam, som mottagaren inte bett om att få.

för att skydda mot störande angrepp. PTS har i sitt förslag till strategi pekat på ett antal frågeställningar om säkerheten i Internets infrastruktur som aktörer inom Internets infrastruktur måste kunna besvara för att leverera efterfrågade tjänster med tillfredsställande tillgänglighet och kvalitet:

- Vilka är kraven på överföringen (volym, snabbhet, säkerhet, ekonomi)?
- Vilken reservkapacitet för bandbredd och processorkraft krävs?
- Vilka alternativa förbindelser eller transmissionsmetoder finns?
- Vad kostar ett kortare respektive längre avbrott i nätet?
- Vilka andra konsekvenser får ett avbrott?
- Hur långa avbrott kan accepteras?
- Hur uppfyller olika alternativ de ställda kraven?
- Vilka standarder ska följas?
- Vilka är riskerna i det valda alternativet?
- Vilka typer av proaktiva eller reaktiva åtgärder ska man vidta för att förhindra eller möta störningar?
- Hur ska katastrof- och kontinuitetsplaneringen utformas och övas?

För att kunna bedöma behovet av åtgärder måste enligt PTS först preciserade krav ställas på driftssäkerhet, framkomlighet, tillgänglighet, äkthet, förändringsskydd och i förekommande fall sekretess. Ansvaret för säkerheten är delat mellan flera olika aktörer. Inte minst användarna har ett ansvar för säkerheten i sin miljö och sitt beteende på Internet.

Dagens allt snabbare anslutningar till Internet kan medföra att användare med bristande kunskaper om riskerna har tillgång till allt kraftfullare plattformer som en angripare kan utgå ifrån när det gäller attacker, spridning av spam med mera. Konsekvensen blir att inte enbart användarens integritet och säkerhet påverkas, utan hela nätverket. Utvecklingen mot att tillhandahålla allt snabbare Internetuppkopplingar, och samtidigt helt och fullt överlåta ansvaret på användaren för säkerheten, är från denna utgångspunkt otillfredsställande.

Operatörerna bör därför ges både en större möjlighet och en större skyldighet att vidta förebyggande åtgärder för att begränsa riskerna för Internets säkerhet. Åtgärderna bör främst syfta till att skydda Internets infrastruktur. Hit hör också att skydda mot avbrott och störningar i elförsörjningen. Beroende på hur känslig utrustningen

är kan ett kort strömavbrott ge upphov till långvariga funktionsstörningar i Internet om inte reservkapacitet finns. De fysiska skyddsåtgärderna för ett säkrare Internet sammanfaller i stor utsträckning med åtgärderna för säkrare telesystem.

Domännamnssystemet (DNS) har en stor betydelse för det logiska skyddet av Internet. Utan tillgång till DNS försvåras eller omöjliggörs användningen av Internet. Utan DNS kan inte en angiven webbadress översättas till de IP-adresser som Internet använder för att styra trafiken till rätt ställe. Falsk DNS-information kan orsaka att trafik styrs fel, vilket kan medföra att e-post eller transaktioner inte fungerar. Det är därför viktigt att säkerställa att informationen i DNS kommer från rätt källa. Hittillsvarande tekniska lösningar har inte kunnat garantera korrekthet eller äkthet. Det finns nu en standardiserad teknik för en säkrare hantering av DNS-information som ger användaren möjlighet att kryptografiskt verifiera korrektheten. Härigenom kan även vissa attacker upptäckas och avvisas. För att öka säkerheten kan den standardiserade tekniken (DNSSEC) användas för att distribuera kryptografiska nycklar för olika tillämpningar.

Belastningsattacker på DNS kan orsakas av att någon ställer upprepade frågor i stor mängd i illvilligt syfte. Överbelastningsattacker förväntas enligt PTS bli vanligare och mer sofistikerade varför även skyddet mot dessa måste vidareutvecklas. Det beror bland annat på användarnas ökade bandbredd och på att mängden exponerade användare har ökat. Även attacker mot programvara med säkerhetshål sker i ökande takt.

Med nästa generation av Internet Protocol (IPv6) blir utbudet av IP-adresser mycket stort och IP-paket som sänds kan förses med inbyggd säkerhet. Genom att en färdig standard för säker IP-kommunikation integreras i protokollet, kommer det att finnas möjligheter att kryptera informationen och säkerställa att den inte kan förvanskas utan att det kan upptäckas. Under de närmaste åren finns dock inget större behov av fler IP-adresser eftersom det i nuvarande version finns drygt en tredjedel kvar av de fyra miljarderna teoretiska IP-adresserna.

Även robust tid är, som framhålls i PTS-rapporten, en förutsättning för att informationshantering i olika former ska kunna upprätthållas och utvecklas. Behovet av spårbarhet i informationstransaktioner kommer att öka i framtiden. Att tid (Universal Time Coordinated, UTC) är tillgänglig och sprids på ett stabilt sätt i Sverige är därför ytterst viktigt. Funktionaliteten i Internet är

beroende av tillgång till korrekt tid. Ofta krävs att olika delar av kommunikationsnäten och IT-systemen är inbördes synkroniserade. I annat fall kan informationsutbyte gå fel, avbrytas eller inte tas om hand på ett korrekt sätt.

I propositionen prop. 1999/2000:86 Ett informationssamhälle för alla uttalade regeringen att den svenska delen av Internet skall kunna drivas oberoende av funktioner utomlands. Tillgång till en säker och internationellt spårbar tidhållning i Sverige med mycket hög och väl dokumenterad kvalitet är därvid en viktig gemensam resurs som staten bör tillhandahålla. Flera åtgärder har vidtagits för att öka robustheten i tidssystemet.

Övriga faktorer som lyfts fram i PTS-rapporten är bristen på säkerhetsmedvetande hos beställare och användare, bristen på samordning utifrån en helhetssyn på forskningsinsatser och bristande samverkan nationellt och internationellt. Dessa behandlas av utredningen i senare kapitel.

Målet bör vara att säkerställa de viktiga funktionerna i Internets infrastruktur, som vid bortfall kan medföra omfattande störningar eller avbrott som försvårar eller förhindrar användning av Internet för stora grupper av enskilda användare eller för viktiga företag, myndigheter och organisationer.

4.2.4 E-legitimationer och certifikat

Användningen av olika tekniker och metoder för säker och skyddad dialog och kommunikation via IKT (informations- och kommunikationsteknik), främst Internet, har ökat kraftigt i Sverige under de senaste åren. En av de främsta drivkrafterna bakom detta är bankernas satsningar på Bank över Internet. Denna utveckling har bland annat möjliggjort framväxten av nya affärsformer inom bank och finans med så kallade nischbanker som helt bygger på kundkontakter via Internet.

I dag har mer än hälften av den svenska befolkningen skaffat någon form av tillgång till sin bank via Internet. Detta innebär att en stor del av den svenska befolkningen kan visa upp ett certifikat och legitimera sig i en dialog över Internet. De lösningar som mest används för Bank över Internet ger en relativt säker metod för identifikation och skyddad kommunikation. Metoderna är emellertid oftast av en ”symmetrisk natur” och därmed knutna till kontak-

ter med den som certifierat och kan inte användas för att åstadkomma strikt personliga generella underskrifter.

Den metod som nu används och där bankerna utfärdar asymmetriska elektroniska legitimationer, baserade på den identifikation som utförts för Bank över Internet, har visat sig vara bättre anpassad för de stora, centrala myndigheterna än för regionala och lokala myndigheter (se avsnitt 2.4.2). Dessa har svårt att få kontroll över, och lönsamhet i, en användning av elektroniska legitimationer. Utredningen anser att bättre information och marknadsföring kring denna typ av tjänster är nödvändig. Inom ramen för utvecklingen av 24-timmarsmyndigheten pågår aktivitet för att skapa acceptabla ekonomiska förutsättningar för e-legitimationer.

4.3 Behovet av operativ förmåga

De resonemang som utredningen för i de tidigare avsnitten väcker frågan om vilka olika förmågor som bör finnas. Skall en systemägare omedelbart kunna reagera om systemet utsätts för en IT-attack eller annat IT-relaterat hot? Skall staten kunna bistå med resurser i en sådan situation? Vilken roll och vilket ansvar har näringslivet för att kunna bistå? Om Sverige skall vara en ledande IT-nation erfordras god informationssäkerhet. Kompetent personal är en grundförutsättning för att kunna reagera på angrepp. Regeringen har tidigare understrukit behovet av en förstärkning av underrättelse- och säkerhetstjänsterna.

Det är ett grundläggande samhällsintresse att skydda nationella elektroniska kommunikationsnät och samhällsviktiga informationssystem. Det är inte rimligt att detta ansvar och de krav på nationell kompetens detta ställer endast skall åvila kommersiella företag. Kompetenta myndigheter med ansvar för denna typ av frågor måste på olika sätt bidra till att höja den allmänna förmågan till skydd. Exempel på detta är den tillsyn som bedrivs av Post- och telestyrelsen på teleområdet och den tillsynsverksamhet som bedrivs av Säkerhetspolisen och Försvarsmakten. Men hur effektiv denna verksamhet än är, kan den i dag endast i begränsad utsträckning identifiera och upptäcka om och när kvalificerade aktörer utnyttjar IT för att penetrera svenska informationssystem.

Sverige har under ett stort antal år arbetat med informationssäkerhetsfrågor – både på bredden genom allmän förebyggande verksamhet och på djupet genom utvecklandet av särskilda kompetenser,

till exempel kryptologi – men bristen på systemtänkande och helhetssyn är påtaglig. Informationssäkerhetsfrågor berör hela samhällets funktionsförmåga men problemet i analysen är att helhetsbilden ofta är oklar. Post- och telestyrelsen framför till exempel i sin delrapport (PTS-ER-2004:37) Tänkbara åtgärder för att säkra Internets infrastruktur:

> Samhället blir allt mer beroende av säker och fungerande kommunikation över Internet. Internet är i dag verksamhetskritiskt för näringslivet och en viktig motor för Sveriges tillväxt. Den offentliga sektorn tar även allt större steg mot Internetberoende bl.a. i och med satsningar på 24-timmarsmyndigheter. Samtidigt ökar incidenter i form av bland annat avbrott samt överbelastnings- och intrångsattacker. Om vitala delar av Internet skulle slås ut kan det få stora konsekvenser för samhället. Internet som sådant bedöms till sin natur vara en relativt säker infrastruktur men den generella skyddsnivån ökar inte lika mycket som riskerna. Internets nuvarande säkerhet sätts utifrån operatörernas kommersiella överväganden på en konkurrerande marknad. Utöver denna nivå kan säkerheten kompletteras med t.ex. statligt beslutade och finansierade åtgärder. Ansvaret för säkerheten ligger dock inte enbart på marknaden och staten. Även användarna har ett ansvar för säkerheten i sin miljö och sitt beteende på Internet. Ett av de största hoten mot Internet i dag är bristande säkerhet i användares miljöer vilket leder till att deras datorer kapas och används som plattformar för attacker mot bland annat kritiska delar av Internets infrastruktur.

Det huvudsakliga problemet är att ingen instans, på teknisk nivå, har haft möjlighet att se och analysera helheten i de angrepp som sker. Detta förhållande gäller oavsett vilken typ av aktör som ligger bakom det specifika angreppet. Det finns därför, enligt utredningens uppfattning, starka skäl för att det inom den statliga sfären skall finnas en fortsatt och utvecklad hög teknisk kompetens för kvalificerat stöd i IT-säkerhetsfrågor.

Slutsatserna i dessa frågor (prop. 2001/02:158) byggde på ett resonemang som fördes i Sårbarhets- och säkerhetsutredningen (SOU 2001:41) kring de starka skäl som talar för att staten skall kunna erbjuda en hög teknisk kompetens och ett avancerat tekniskt stöd i IT-säkerhetsfrågor. Sårbarhets- och säkerhetsutredningens motiv för att bygga upp den tekniska informationssäkerheten med ansvar fördelat på funktioner i flera olika myndigheter var att detta bedömdes vara snabbaste vägen att skapa nödvändig kompetens och förmåga inom de olika funktionsområdena. Sårbarhets- och säkerhetsutredningen ansåg att verksamheten efter ett uppbyggnadsskede borde utvärderas också i sin organisatoriska lösning.

Sedan detta resonemang fördes har det, enligt InfoSäkutredningens mening, blivit än mer tydligt att staten måste ha ett antal operativa förmågor inom informationssäkerhetsområdet. Dessa förmågor kan uppnås genom ett starkare och mer sammanhållet statligt engagemang. De förmågor staten måste ha kan beskrivas som:

- Helhetssyn, vilket förutsätter deltagande från underrättelse- och säkerhetstjänsterna
- Förtroende
- Försvars- och säkerhetspolitiskt behov av skydd för känsliga uppgifter
- Garanterad resurs mot framförallt aktörsbundna kvalificerade IT-relaterade hot eller andra IT-säkerhetskritiska situationer
- Förmåga att ingripa mot och hantera kvalificerad IT-relaterad brottslighet
- Behov av analys på olika nivåer
- Garantera och tillvarata unik teknisk kompetens
- Nationellt och internationellt samarbete.

Kravet på förtroende är särskilt stort för säkerhetskritisk teknik för totalförsvaret eller andra kunder i samhället med försvars- eller säkerhetspolitiskt känslig verksamhet. Dessa aktörer kan inte i alla lägen förlita sig på marknaden, utan behöver tillgång till teknisk kompetens inom staten. Beställarkompetensen är avgörande för att skydda sig mot avsiktliga eller oavsiktliga säkerhetsbrister. Insynen i uppgifter av betydelse för rikets säkerhet kan inte alltid lämnas till enskilda aktörer på marknaden.

Staten bör säkerställa tillgång till kvalificerad teknisk kompetens att använda i olika säkerhetskritiska situationer. Staten har ansvar för skyddet mot IT-attacker från främmande land eller annan aktör med hög kompetens, som drabbar Sveriges säkerhet. IT-säkerhet är en viktig komponent i detta skydd, varför staten måste ha en garanterad, kvalificerad teknisk kompetens på detta område, att användas för att förebygga nationella kriser med IT-inslag eller till att snabbt ta fram skydd mot elakartade program och för att testa säkerheten i verksamheter av stor betydelse för samhällets funktionsförmåga.

Kunskaper måste finnas både på ett allmänt plan om tekniska principer för IT-säkerhet och mer specifikt om produkter på marknaden. De tekniska detaljkunskaperna om produkter, protokoll, kända tekniska säkerhetsbrister och virus m.m. måste också vara

aktuella. Till detta kommer nödvändigheten av att inom en och samma organisation spänna över flera olika IT-verksamhetsområden för att kunna se helheten i olika problem.

De metoder som signalspaningen har utvecklat under lång tid är av avgörande betydelse för att vi nu och i framtiden ska kunna värja oss mot framför allt olika typer av aktörsrelaterade teknogena hot. Ett bra historiskt exempel på detta är det förhållande som utvecklats mellan den kryptologiska forceringsverksamheten vid Försvarets radioanstalt (FRA) och den traditionella signalskyddsverksamheten vid Totalförsvarets signalskyddssamordning (TSA). Ett liknande förhållande har under de senaste åren uppstått vad avser den kunskap som signalspaningsverksamheten har utvecklat i fråga om brister i IT-system. Denna kunskap har uppstått såväl genom den traditionella signalspaningsverksamheten som ur de IT-kontroller som sker i Försvarets radioanstalts regi. Vad som ytterligare understryker signalspaningens unika förmåga att bistå är att allt fler IT-system innehåller inbäddade kryptografiska funktioner, vilket ställer krav på kompetens vad avser såväl kryptologi som hög IT-säkerhetskompetens.

Vikten av god kryptologisk förmåga som nationell resurs kvarstår och har förstärkts i och med att allt fler samhällskritiska funktioner blir beroende av kryptologisk funktionalitet. Grundförutsättningen för detta är stabil och tillräcklig kompetens och goda arbetsredskap i form av beräkningskraft, som hela tiden utvecklas genom att forcera nya kryptosystem.

Den tekniska komplexiteten ökar hela tiden, parallellt med beroendet av IT-system. I många IT-system finns i dag kryptologiska funktioner inbyggda. Det gör att behovet av att besitta både hög IT-förmåga och kryptologisk spetskompetens har tillkommit.

För att kunna fullgöra uppgiften att vara en resurs av hög kvalitet för samhället avseende teknisk informationssäkerhet krävs att de ansvariga för denna typ av verksamhet kontinuerligt inhämtar relevant information genom eget arbete och genom kontakter, såväl nationellt som internationellt. Detta kräver i sin tur att man har ett stort förtroende och tillgång till ett nätverk av samarbetspartners nationellt och internationellt.

Samarbete med andra organisationer på IT-säkerhetsområdet är av yttersta vikt. Samarbete ger högre effektivitet genom att man kan dela på arbetet och dra fördelar av det andra gjort. Nationellt finns det ett stort behov av att sprida kunskap om tekniska brister i olika IT-system. Detta är inte lika självklart när det gäller den

internationella dimensionen då man på detta sätt riskerar att blottlägga nationella brister.

Det är av avgörande betydelse att det finns ett förtroende från den offentliga sektorn såväl som från andra verksamhetsområden på nationell nivå. Förtroendet skiljer sig i dag mellan olika sektorer.

Datakommunikation är en global och gränslös företeelse. Därav följer att IT-säkerhet i högsta grad är en internationell fråga. Problemen är oftast likartade världen över, vilket motiverar ett långtgående internationellt samarbete. Sverige måste delta i de internationella nätverk som finns och bildas på området. Endast en statlig aktör med hög IT-säkerhetskompetens kan delta i dessa nätverk och aktivt tillföra kunnande i arbetet. Detta kan gälla utbyte av metodik och erfarenheter, samarbete om analys av elakartade program eller överenskommelser om evalueringskriterier. Skulle sedan 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.

En numera viktig och central fråga är vad Sverige kan bidra med på detta område inom EU, så att säkerheten även där kontinuerligt förbättras. Det är utredningens uppfattning att Sverige måste säkerställa en hög teknisk kompetens också för att vara en aktiv aktör och en attraktiv partner i olika EU sammanhang. Ett exempel på detta är att Sverige under de senaste åren vid ett flertal tillfällen blivit tillfrågat om att genomföra en andra evaluering av signalskyddsprodukter från andra stater. Inom den Europeiska Unionen har ett regelverk utarbetats för att bland annat tillförsäkra en opartisk andrahandsevaluering av kryptografiska produkter. Denna evaluering skall utföras av en godkänd myndighet, en s.k. *Appropriately Qualified Authority* (AQUA). Detta arbete är omfattande vad avser själva evalueringen. I processen ingår bland annat att verifiera även andra delar än de rent kryptografiska, såsom mätning av röjande signaler och viss kodgranskning av säkerhetskritiska funktioner. Regelverk ställer bland annat krav på att ett kryptosystem skall vara godkänt av behörig myndighet i det land som offererar kryptoprodukten. Dessutom skall en AQUA i en annan medlemsstat med motsvarande förmåga genomföra en s.k. andrahandsevaluering. Sverige har 2004 ansökt om att bli godkänt enligt detta regelverk. För svensk kryptoindustri innebär detta att dess produkter måste vara nationellt godkända för att kunna offereras i vissa samanhang. I dag finns ingen formellt utsedd myndighet för att hantera dessa

frågor eftersom TSA endast har mandat att godkänna produkter för totalförsvarets behov.

En viktig fråga är om staten bör tillhandahålla analysfunktioner för att kunna analysera incidenter. Syftet med sådana funktioner är att kunna dra erfarenheter av händelser som skett och på så sätt kunna anpassa planer och metoder efter detta. De aktiviteter staten bedriver inom området bör syfta till att värna såväl statens egen verksamhet som verksamhet inom kommuner, landsting och näringsliv. En bärande verksamhetsidé bör därför vara att, i möjligaste mån och inom ramen för gällande lagstiftning, sprida resultat.

Förmågan att kunna analysera incidenter tillhandahålls av flera delar inom statsförvaltningen beroende på hur man definierar termen analys. En teknisk analys av en incident ställer frågorna vilken sårbarhet har utnyttjats, vilken metod har använts, vilken är den tekniska måltavlan och vilka tekniska konsekvenser medför incidenten. Aktören eller dennes motiv är av underordnat intresse i en teknisk analys.

Aktörs- och motivanalyser genomförs av rättsväsendet, underrättelsetjänsterna och i forskningssammanhang. En polisiär analys av en incident koncentreras närmast kring aktören och dennes motiv och den tekniska analysen kan förenklat beskrivas som bevissäkring. Underrättelsetjänsternas och forskningens analyser av aktör och motiv torde i mycket ringa mån koncentreras kring den tekniska analysen annat än som ett av flera spelmoment.

PTS/Sitic genomför tekniska analyser vars resultat publiceras brett i syfte att kunna informera samhällets organisationer om nya problem som kan störa IT-system samt att kunna lämna information och råd om förebyggande åtgärder. Rättsväsendet genomför tekniska analyser i syfte att säkra bevis. FRA genomför teknisk analys i syfte att kunna stödja individuella organisationers arbete med informationssäkerhet.

Även när det gäller förmågan att kunna respondera vid incidenter är detta en vital funktion. Om Sverige inte själv har denna förmåga kommer vi att vara beroende av andras förmåga. Det är då tveksamt om vi kommer att erhålla information för att kunna vidtaga åtgärder. Det finns också ett väl etablerat kontaktnät mellan olika länders responsfunktioner. På detta sätt kan Sverige både erhålla samt lämna information. Förmågan att kunna respondera vid incidenter tillhandahålls av flera delar av statsförvaltningen. PTS responderar genom att varna och ge upplysning om skydd till samhällets organisationer. Rättsväsendet responderar genom att avbryta, utreda

och/eller lagföra incidenter. FRA responderar genom att individuellt stödja organisationer som har drabbats av incidenter och ska också kunna stödja insatser vid nationella kriser med IT-inslag.

Certifieringsorganet vid FMV (CSEC) granskar och godkänner utvärdering av IT-säkerhet i produkter i enlighet med Common Criteria. Erfarenheter från rapporterade incidenter kan påverka det svenska regelverket för hur produkterna granskas. Detta kan bidra till att erfarenheterna från incidenter förs vidare till produktutvecklarna, vilket i sin tur på sikt leder till en ökande tillgång på motståndskraftiga produkter.

En synpunkt som från flera håll har framförts till utredningen är att respons- respektive analysfunktioner skulle vara aktiva året runt 24 timmar, 7 dagar i veckan. Relevansen i en sådan konstruktion skiljer sig mellan olika aktiviteter såsom incidentrapporthantering, respons, analys och tekniska respektive polisiära ansvar. Det finns i dag inom rättsväsendet en operativ dygnetruntberedskap vid Rikskriminalpolisens IT-brottsrotel för brottsrelaterade IT-incidenter. Roteln är Sveriges kontaktpunkt inom ramen för G8-överenskommelsen och ingår även i Interpols kontaktorganisation för så kallat high-tech crime.

Inom polisen finns även en samordningsfunktion med inriktning mot brottsrelaterade IT-incidenter (S-BIT). Funktionen är bemannad med personal från Rikskriminalpolisen och Säkerhetspolisen. Funktionen utgör en central ingång för den som behöver komma i kontakt med polisen med anledning av en misstänkt brottslig IT-incident. Funktionen skall ha lägesöverblick och bedriva kriminalunderrättelseverksamhet. Den utgör polisens kontaktyta mot andra aktörer i samhället som har uppgifter inom informationssäkerhetsområdet. Funktionen bedriver också brottsförebyggande verksamhet genom bl.a. föreläsningar och utbildningar, samt sammanställer och sprider information inom ämnesområdet.

Utredningen tar i detta betänkande inte ställning till hur de olika förmågor som beskrivits ovan skall organiseras men återkommer i slutbetänkandet till organisatoriska förslag.

4.4 Kriterier för samhällsviktiga verksamheter och system

Ett begrepp som har visat sig grundläggande i utredningsarbetet är *samhällsviktig verksamhet*. I diskussionen om vad som utgör det offentliga åtagandet är begreppet återkommande. Enligt vad utredningen kunnat få fram finns dock inte någon generellt vedertagen definition av begreppet. Sannolikt är det så att det finns en mängd olika verksamheter som vid ett givet tillfälle kan vara mer eller mindre viktiga för staten. Staten kan således ha ett ökat intresse av att säkerheten upprätthålls i sådana verksamheter.

Det finns i dag inga av statsmakterna beslutade kriterier för vilka verksamheter, tekniska system och därtill kopplade funktioner som är att betrakta som samhällsviktiga. Det är därför svårt för myndigheter med föreskrivande/rådgivande uppgifter att utkräva de högre säkerhetskrav som borde åvila de ansvariga för samhällsviktiga system. Det faktum att det i dag inte finns dokumenterat vilka verksamheter och system som är att betrakta som särskilt viktiga för samhället, och att denna centrala fråga därmed omgärdas av ett stort tolkningsutrymme, kan delvis ha sin grund i att det råder osäkerhet om hur begreppet ”samhällsviktig” skall definieras. Det kan också bero på att den viktiga uppgiften att ta fram en förteckning aldrig har delegerats till någon enskild, utpekad aktör utöver de myndigheter som ingår i Krisberedskapsmyndighetens samverkansområden.

Det kan och bör ställas krav på kriterier för vad som är att betrakta som samhällsviktiga verksamheter och system. Då den tekniska utvecklingen snabbt går framåt kan inte tekniken i sig vara styrande vid upprättandet av kriterier. Snarare bör kriterierna tas fram genom beaktandet av vilken typ av verksamhet som är särskilt viktig för samhället samt med kännedom om tekniska och systemrelaterade ömsesidiga beroendeförhållanden. Samtidigt finns det motiv för ett pragmatiskt angreppssätt i syfte att underlätta för myndigheter att successivt förbättra samordning och samverkan inom säkerhetsarbetet. Det primära torde vara att bättre precisera inom vilka verksamhetsområden och hos vilka aktörer som det kan finnas skäl för statsmakterna att ställa särskilda krav när det gäller exempelvis informationssäkerhet.

Utredningens överväganden om gränsdragningen mellan det privata och det offentliga åtagandet visar att det finns områden där en sådan gräns är svår att dra. Ett tydligt sådant område är infra-

strukturen, till exempel el- och teleinfrastruktursystemen för elöverföring och –distribution samt telekommunikation, som båda är mycket viktiga för samhällets funktion och där det finns starka motiv för att ställa särskilda krav på leveranssäkerhet och kvalitet. Begreppet samhällsviktig är således relevant i dessa sammanhang. Staten har inom ramen för samhällets beredskap också möjligheter att bidra ekonomiskt till säkerhetshöjande åtgärder. Den för samhället viktiga infrastrukturen är ofta i privat eller kommunal ägo. Detta begränsar i dag statens möjligheter att i formell, administrativ mening ställa krav utöver vad som motiveras av beredskapsskäl. Sådana extra krav på säkerhet kan således bara ske med stöd av en ny lag. Underlag för någon form av legal definition av begreppet samhällsviktig vore mot denna bakgrund önskvärd för det fortsatta författningsarbetet.

I lagen (1990:217) om skydd av samhällsviktiga anläggningar används begreppet samhällsviktig. I lagen definieras dock inte vad som är en samhällsviktig anläggning. Däremot följer det av bestämmelsen om vad som får förklaras som skyddsobjekt vad som kan anses vara en sådan anläggning, i praktiken sådana anläggningar, militära och civila, som är av särskild betydelse för totalförsvaret. I lagen finns vissa bestämmelser för tillträdesbegränsning och bevakning. Enligt utredningens mening lämnar denna lag inte tillräckligt stöd för en utvidgad användning av begreppet samhällsviktig.

Mot denna bakgrund har utredningen uppdragit åt Totalförsvarets forskningsinstitut (FOI) att utarbeta kriterier för bedömning om en verksamhet är samhällsviktig eller inte. Sådana kriterier skulle kunna underlätta för enskilda verksamhets- och systemägare att själva avgöra om eller i vilken grad som deras verksamheter eller system är att betrakta som samhällsviktiga. Kriterierna skulle också kunna tjäna som underlag för staten att lämna stöd till förebyggande och förberedande insatser, att prioritera resurser för ökad informationssäkerhet och för kravställande i framtiden.

FOI har presenterat en modell, ett processverktyg, som ger vissa riktlinjer för berörda aktörer. Den är tänkt att kunna användas på flera olika nivåer, från delar av enskilda företag till hela branscher och myndigheter. Modellen är också avsedd att kunna användas av både offentliga och privata aktörer med centrala, regionala eller lokala perspektiv. Den presenterade modellen bör även, i utvecklad form, kunna användas vid styrning, uppföljning och tillsyn.

Kriteriemodellen tar sin utgångspunkt i ett resonemang om samhällets grundläggande värden så som dessa uttalats i olika politiska

sammanhang. Utredningen har noterat att de begrepp som FOI använder också har använts i förarbeten till delar av den grundläggande lagstiftning som gränsar till utredningens område. I FOI:s dokument redovisas och tolkas dessa värden som omfattar bland annat respekt för människans värdighet, frihet, demokrati, jämlikhet, rättstatsprincipen och respekt för de mänskliga rättigheterna. Dessa grundläggande värden tolkas och konkretiseras därefter i vad FOI benämner samhällets vitala intressen. Dessa intressen utgör sedan basen för att kunna bedöma samhällsviktigheten i en verksamhet. Verksamheten skall således betraktas som samhällsviktig om ett bortfall eller en störning av denna skulle medföra allvarliga konsekvenser för möjligheterna att tillgodose samhällets vitala intressen. FOI visar vidare ett resonemang om en kriteriemodell för bedömning av verksamheters vikt för samhället. De kriterier som lyfts fram är olika aspekter av konsekvenser som intensitet, omfattning och utbredning samt, aspekter av tids- och orsakskriterierer. Modellen tar även hänsyn till bedömningar av hur unik en enskild verksamhet är samt dess beroenden av andra verksamheter. Beroendeaspekten är av intresse eftersom en verksamhet som inte anses vara viktig i sig, kan bli det om andra verksamheter visar sig vara beroende av den.

Utredningen konstaterar att behovet av att definiera samhällsviktig verksamhet även gäller den del av den tekniska infrastrukturen, till exempel inom elsystemet, telefunktionerna och infrastrukturen för Internet som är avgörande för samhällets funktionsförmåga. Om bortfall av kapacitet och förmåga sker i en omfattning som utgör hot mot liv och hälsa eller allvarligt kan skada vitala ekonomiska eller andra angelägna samhällsintressen, kan en verksamhet beskrivas som samhällsviktig. Särskilt måste ömsesidiga beroendeförhållanden tillmätas betydelse i sådana fall.

FOI har betonat att modellen har tagits fram under mycket kort tid och att mycket arbete återstår. Det har till exempel inte funnits tid att pröva modellen i en vidare krets av aktörer och det har därför inte varit möjligt att förankra resonemangen. Enligt utredningens mening är dock FOI:s arbete, trots angivna reservationer, av så grundläggande karaktär att det bör kunna ligga till grund för fortsatt arbete med att finna användbara kriterier för identifiering av samhällsviktiga verksamheter och system. Utredningen har erfarit att regeringen beslutat, utifrån den redovisning som Krisberedskapsmyndigheten (KBM) har lämnat i mars 2005, inom vilka samhällsområden det bör finnas en förstärkt fredstida förmåga och

att Krisberedskapsmyndigheten (KBM) i samverkan med de myndigheter som anges i förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap skall påbörja ett arbete med att närmare definiera vad som avses som samhällsviktig verksamhet. Redovisning skall ske den 31 januari 2006. FOI:s arbete bör därför drivas vidare och förslagsvis samordnas med KBM:s arbete inom ramen för regeringsuppdraget.

Utredningen har för avsikt att överlämna FOI:s rapport till regeringen i samband med slutbetänkandet.

4.5 Utredningens slutsatser av behovet av strategi och konkreta åtgärder

Enligt regeringens översiktliga strategi enligt proposition 2001/02:158 Samhället säkerhet och beredskap, skall störningar i samhällsviktig verksamhet kunna *förhindras* eller *hanteras*. Underrättelse- och säkerhetstjänstens arbete bör *förstärkas*. Utredningen anser att detta är en riktig utgångspunkt men att det finns motiv för en fördjupning och tillägg till det skrivna. Störningar i samhällsviktig verksamhet bör kunna *förebyggas* och *förberedelse* för att minimera konsekvenserna bör bedrivas.

Mot bakgrund av de resonemang som redovisas i kapitel 3 och 4, föreslår utredningen en strategi som innefattar att:

1. utveckla Sveriges position inom EU och i internationella sammanhang
2. skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet
3. främja ökad användning av IT
4. förebygga och kunna hantera störningar i informations- och kommunikationssystem
5. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen
6. förstärka förmågan inom området nationell säkerhet

I strategin bör även ingå att:

7. utnyttja samhällets samlade kapacitet
8. fokusera på samhällsviktig verksamhet
9. öka medvetenheten om säkerhetsrisker och möjligheter till skydd
10. säkerställa kompetensförsörjningen

För att kunna genomföra intentionen i den nationella strategin bör ytterligare åtgärder föreslås. En springande punkt i de åtgärder som bör vidtas snarast är att öka förtroendet för IT. Detta kan ske genom att öka kunskaperna om de risker och hot som finns samt vilka åtgärder som kan vidtas. Utredningen anser att dessa åtgärder måste ske på en bred front. Det gäller att öka kunnandet i alla delar av samhället.

Utredningen konstaterar att staten behöver egen och unik kompetens. Dels har staten krav på sig att ta ansvar för samhället oavsett konjunkturer och dels har staten det yttersta ansvaret för den nationella säkerheten, vilket ställer särskilda krav.

Det krävs ömsesidigt informationsutbyte och samarbete mellan den offentliga sektorn och näringslivet. Utredningen konstaterar att Sverige i dag inte har tillräckliga resurser för att bygga dubbla strukturer.

Utredningen konstaterar att det behövs bättre rutiner att tillvara den information som i dag finns i underrättelseorganen. Dessa myndigheter har en unik kompetens och använder sig av unika metoder, men det måste säkerställas att den information de inhämtar inte stannar hos dem. Metoder för delgivning bör utvecklas för att kunna ge en helhetsbild av de risker och hot som finns inom IT-världen.

Utredningen anser att det bör finnas en funktion för analys av de incidenter som förekommer, för att vi ska kunna dra slutsatser av dessa. Det bör också finnas en responsfunktion. Hur dessa funktioner skall organiseras kommer utredningen att återkomma till i slutbetänkandet.

5 Den internationella dimensionen

5.1 Inledande kommentar om säkerhetsproblemets internationella dimension

Då enskilda användare i allt högre utsträckning är beroende av sammankopplade lokala och globala informationssystem och kommunikationsnät, är ansvaret för säkerheten i dessa av central betydelse. Mycket av det arbete som genomförs inom EU syftar därför till att öka nät- och informationssäkerheten och stärker därigenom integriteten och ökar tillgängligheten. Detta är viktigt för tillväxten, konkurrensen och utvecklingen av demokratin. OECD bedriver utvecklingsarbete inom ramen för sina olika kommittéer. Länderna har också enats om riktlinjer för nät- och informationssäkerhet, vars syfte är att etablera en säkerhetskultur på området.

Att bekämpa hoten mot informationssystemen är inte bara en svensk angelägenhet, utan är av global natur. Därför krävs internationell samverkan, både i fråga om underrättelseinhämtning och brottsbekämpning.

I kapitel 4 redovisas vissa utgångspunkter för hur den nationella strategin kan utvecklas. Enligt utredningens mening kan dock nationella problemen inte lösas enbart med nationella medel. Det går heller inte alltid att med nationell reglering komma åt problemkällorna, då dessa ofta har en internationell bakgrund. Det borde således inte vara någon större nyhet att även utredningen ansluter sig till detta synsätt, det vill säga att informationssäkerheten har en internationell dimension. Svenska intressen på informationssäkerhetsområdet måste därför också bevakas så att säga utomlands.

En stor del av Sveriges internationella samarbete inom informationssäkerhetsområdet, sker i olika bilaterala former. Flera myndigheter har mycket viktiga kontakter med motsvarande myndigheter i andra länder, inom och utom EU. Samarbete finns inom flera

områden från de rent tekniska frågorna till mer övergripande policyfrågor.

Utredningen kan konstatera att sedan publicerandet av det andra delbetänkandet har arbetet med informationssäkerhet gått framåt inom flera olika områden inom EU. Det internationella utbytet på informationssäkerhetsområdet från svenskt håll har dock varit splittrat och inte i tillräcklig utsträckning samordnat på nationell nivå. För att Sverige skall ha fortsatt gott genomslag inom området måste även det internationella utbytet samordnas, precis som svenska ställningstaganden i policyfrågor.

Utredningen har uppdragit åt KBM att göra jämförelser med hur andra länder har hanterat informationssäkerhetsfrågorna, bland annat olik sätt att organisera säkerhetsarbetet. Utredningen avser därför att återkomma till dessa frågor i slutbetänkandet september 2005.

5.2 Samverkan inom EU

Utredningen kunde redan i sitt andra delbetänkande konstatera att det inom EU sker ett arbete där medlemsländerna närmar sig varandra både vad gäller lagstiftning och vad gäller synen på och hanteringen av informationssäkerhetsproblematiken. De olika dimensionerna av detta arbete har även berörts ovan i avsnitt 1.5. Arbetet sker huvudsakligen i medlemsländernas intresse men EU som organisation har också ett eget intresse av att skydda sin sekretessbelagda information. De flesta initiativ med koppling till informationssäkerhet, som tagits inom EU, faller inom det som kallas EU:s första pelare (den Europeiska Gemenskapen) och tredje pelare (rättsliga- och inrikes frågor). Endast i liten utsträckning hittar man initiativ inom den andra pelaren (den gemensamma utrikes- och säkerhetspolitiken). Utgångspunkten för de informationssäkerhetsrelaterade projekten synes främst vara främjande av handeln, och i förlängningen att alla i medlemsländerna skall ha tillgång till informationstekniken och ha IT-kompetens. En sådan ambition förutsätter implicit en ökad grad av nät- och informationssäkerhet. Projektet e-Europa presenterades av kommissionen redan 1999 och kan ses som ett ramverk för IT-utvecklingen inom EU. De säkerhetsrelaterade aspekterna som sprungit ur projektet har sin utgångspunkt i bland annat behovet av att bygga förtroende för den elektroniska handeln, inklusive införandet av smarta kort.

Bland åtgärderna återfanns bland annat olika former av certifiering och stimulerandet av privat-offentligt samarbete kring pålitliga nät. Även kampen mot högteknologisk brottslighet inom unionens tredje pelare kan anföras som en åtgärd för att stärka förtroendet för nyttjandet av Internet för varor och tjänster. Samtidigt har unionen som ett självständigt mål att skapa ett område med frihet, säkerhet och rättvisa. Åtgärder mot all brottslighet, inklusive IT-relaterad sådan, är en viktig del.

Utredningen gjorde i sitt andra delbetänkande en översiktlig redogörelse för det arbete som har bedrivits inom EU på informationssäkerhetsområdet de senaste åren. Utredningen kan konstatera att sedan publicerandet av det delbetänkandet har arbetet med informationssäkerhet gått framåt inom flera olika områden. Sedan i mars 2004 finns Europeiska nät- och informationssäkerhetsbyrån (Enisa) som behandlar informationssäkerhetsfrågor. På integritetsområdet diskuteras bland annat frågan om uppgiftsskyddsombud och deras uppgifter. Kommissionen har vid ett flertal tillfällen återkommit till frågan om elektroniska signaturer, bland annat vid halvtidsöversynen av e-Europa 2005 och vid uppdateringen av handlingsplanen för samma projekt. I kampen mot IT-brottsligheten har rådet antagit ett rambeslut med syftet att tillnärma medlemsstaternas strafflagstiftning när det gäller angrepp mot informationssystem. Samtidigt förhandlas ett rambeslut som syftar till att tillse att uppgifter om Internet- och teletrafik - vilka uppkopplingar som stått i förbindelse med varandra vid en viss tidpunkt - bevaras under en viss tid för att finnas tillgängliga för brottsbekämpande myndigheter vid utredningar av brott.

Utredningen konstaterade i sitt andra delbetänkande att internationellt utbyte på informationssäkerhetsområdet från svenskt håll har varit splittrat och inte i tillräcklig utsträckning samordnat på nationell nivå. För att Sverige skall ha fortsatt gott genomslag inom området måste även det internationella utbytet samordnas, precis som svenska ställningstaganden i policyfrågor.

Mycket av vad som pågår inom EU med bäring på informationssäkerheten är av policykaraktär och rör till exempel tillnärmning av medlemsstaternas lagstiftning. Värda att nämnas är dock även de initiativ inom EU som rör mer operativ samverkan. Inom första pelaren finns framför allt Enisa som skall främja gemenskapens, medlemsstaternas, och som en följd av detta, näringslivets förmåga att förhindra och lösa problem som rör nät- och informationssäkerhet. På tredje pelarens område finns Europol, där medlems-

staterna sedan 1999 samverkat i kampen mot bland annat IT-relaterad brottslighet. Det under generalsekretariatet placerade gemensamma situationscentret, SITCEN, har ett mandat att analysera underrättelser och öppen information i syfte att stödja generalsekretariatet.

Nät- och informationssäkerhet

Sverige förde upp frågan om informationssäkerhet på EU:s dagordning under det svenska ordförandeskapet. I Europeiska rådets slutsatser från mötet i Stockholm den 23–24 mars 2001 framgick det att rådet tillsammans med kommissionen skulle ”utarbeta en övergripande strategi för säkerheten när det gäller elektroniska nätverk tillsammans med praktiska åtgärder för genomförande. Detta bör läggas fram i god tid inför Europeiska rådets möte i Göteborg.” Meddelandet Nät- och informationssäkerhet: förslag till en europeisk strategi är kommissionens svar på denna uppmaning.

Kommissionens meddelande beskriver de hot som finns mot elektroniska nätverk och informationssystem och föreslår en strategi och en rad åtgärder för hur man på europeisk nivå skall komma tillrätta med dessa problem.

Kommissionens meddelande följdes även av två resolutioner om informationssäkerhet: om en gemensam inställning och särskilda åtgärder på området för nät- och informationssäkerhet (EUT C43 28.1.2002, s. 2) samt om en europeisk strategi för nät- och informationssäkerhet (EUT C48, 18.2.2003, s. 1).

I resolutionen från januari 2002 välkomnade medlemsstaterna kommissionens förslag att inrätta en specialgrupp om informationssäkerhet. Som en följd av detta presenterade kommissionen förslaget som efter förhandlingar i rådet och Europaparlamentet ledde till förordningen om Enisa.

Enisa skall ha som mål

- att förbättra gemenskapens, medlemsstaternas och näringslivets förmåga att förhindra, ta i tu med och lösa problem som rör nät- och informationssäkerhet,
- att ge stöd och råd till kommissionen och medlemsstaterna i frågor om nät- och informationssäkerhet,
- att utveckla – på grundval av såväl nationella insatser som gemenskapsinsatser – en hög nivå av sakkunskap och utnyttja denna

till att främja ett brett samarbete mellan offentliga och privata aktörer,
- att bistå kommissionen i det tekniska förberedelsearbetet för uppdatering och utveckling av gemenskapslagstiftningen på området nät- och informationssäkerhet.

För att åstadkomma detta ges byrån bland annat följande uppgifter:

- Samla in lämplig information för analys av befintliga och nya risker.
- Ge EU:s institutioner råd inom byråns verksamhetsområde.
- Förbättra samarbetet mellan olika aktörer inom nät- och informationssäkerhetsområdet (näringsliv, akademi, offentliga etc.).
- Underlätta samarbetet mellan kommissionen och medlemsstaterna för att utveckla gemensamma metoder för att förebygga, ta itu med och reagera på problem inom nät- och informationssäkerhetsområdet.
- Bidra till ökad medvetenhet och sprida information om informationssäkerhetsfrågor.
- Bistå kommissionen och medlemsstater i dialogen med industrin.
- Följa utvecklingen av standarder för produkter och tjänster.
- Ge kommissionen råd om forskning inom verksamhetsområdet.
- Främja åtgärder för riskbedömning, interoperabla lösningar för riskhantering etc.

Byrån ges dock inte någon operativ roll utan är rådgivande. Det påpekas särskilt att den inte skall inkräkta på de nationella regleringsmyndigheternas arbetsuppgifter. Förordningen om Enisa gäller i fem år. Byrån kommer att ha 44 anställda. I styrelsen sitter representanter för medlemsstaterna, kommissionen och representanter för industrin, akademin och konsumentgrupper. Näringsdepartementet representerar Sverige i styrelsen och har bidragit med en nationell expert i startarbetet med Enisa. Svenskar finns även i den ständiga intressentgrupp som skall ge råd till byråns verkställande direktör om det årliga arbetsprogrammet.

Dataskydd och integritet

År 1995 antog Europaparlamentet och rådet direktiv 95/46/EG om skyddet av fysiska personers grundläggande rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter

samt det fria flödet av sådana uppgifter. Direktivet tog även upp behovet av säkerhet och sekretess avseende sådana uppgifters behandling samt den registeransvariges ansvar för ett lämpligt tekniskt och organisatoriskt skydd för uppgifterna mot förstörelse, förlust, manipulering, spridning etc. Genom direktivet inrättades en arbetsgrupp, den så kallade artikel 29-arbetsgruppen, som skall följa upp dataskyddsområdet och årligen avge en rapport. Från svensk sida är Datainspektionens generaldirektör ledamot i arbetsgruppen. Direktivet har genomförts i Sverige genom antagande av den svenska personuppgiftslagen (1998:204) som också inkluderar säkerhetsfrågorna.

Efter direktiv 95/46/EG har ett flertal direktiv hanterat frågor såsom till exempel harmonisering av medlemsstaternas bestämmelser för att säkra en likvärdig nivå på skyddet för de mest grundläggande fri- och rättigheterna, i synnerhet rätten till privatliv, med avseende på behandling av personuppgifter inom telekommunikationsområdet (direktiv 2002/58/EG).

I december 2000 antog Europaparlamentet och rådet en förordning rörande hanterandet av personuppgifter i EU:s gemenskapsorgan (45/2001). Förordningen reglerar säkerhetsfrågor som berör såväl sekretess som säkerhet vid behandling av personuppgifter. Till exempel skall registeransvarig vidta lämpliga säkerhetsåtgärder, inte minst för att hindra obehöriga att få tillgång till datasystemen och förhindra att obehöriga läser eller manipulerar information i lagringsmedier samt för att kunna följa upp vilka som arbetat i systemet etc. Förordningen stadgar också att varje gemenskapsinstitution skall ha ett uppgiftsskyddsombud samt att det på EU-nivå skall finnas en datatillsynsombudsman. Uppgiftsskyddsombudens ansvar, uppgifter och befogenheter har, i ett i september 2004 ännu ej antaget utkast till rådsbeslut, specificerats närmare.

Elektronisk handel och förtroendefrågor

Den gemensamma marknaden är en central fråga för EU. De initiativ som berör konkurrensfrågor inom området elektroniska tjänster och elektronisk handel har ofta också en koppling till olika aspekter av nät- och informationssäkerhet. Inte minst påpekas att säkerheten på nätet har en stor betydelse för konsumenters och andra brukares förtroende för den nya tekniken. Även frågorna kring skydd av personuppgifter och utbredningen av databrottslighet betonas.

År 2002 kom Europaparlamentet och rådet med ett ramdirektiv (2002/21/EG) syftande till ett ”harmoniserat regelverk för elektroniska kommunikationstjänster och kommunikationsnät, tillhörande faciliteter och tjänster”. Direktivet handlade framförallt om att skapa ett regelverk för ett ”ordnat” – ur såväl ekonomisk som teknisk synvinkel – system. I ramdirektivet angavs också tillskapandet av Kommunikationskommittén som skall främja informationsutbytet mellan medlemsstaterna och mellan kommissionen och medlemsstaterna vad avser regleringar inom det aktuella området. I kommittén företräds Sverige av tjänstemän från Näringsdepartementet.

Ramdirektivet angav också uppgifter för de nationella regleringsmyndigheterna, bland annat att de skall bidra till gott skydd för personuppgifter men också säkerställa de allmänna kommunikationsnätens integritet och säkerhet. Dessa regleringsmyndigheter bildade senare Europeiska gruppen för regleringsmyndigheter med uppgift att fungera som rådgivare till kommissionen och som en förmedlande länk mellan nationella regleringsmyndigheter. Svensk nationell regleringsmyndighet är Post- och telestyrelsen.

Frågor om kryptering, certifiering och smarta kort har återkommit i EU:s initiativ. I ett meddelande från 1997 noterade kommissionen att kryptografi är det verktyg som krävs för att garantera säkerhet och förtroende för elektronisk kommunikation, men att det inte finns någon fungerande inre marknad för detta område. Kommissionen föreslog vidare att man skulle inrätta ett ramverk på gemenskapsnivå för digitala signaturer, närmare bestämt genom att ställa upp gemensamma kriterier för certifiering, och stimulera en europeisk industri för kryptografiska tjänster och produkter. Rådets slutsatser med anledning av detta meddelande noterade betydelsen av tjänster inom området kryptering och certifiering men pekade också på känsligheten med krypterad kommunikation, inte minst då den kan utnyttjas av brottsligheten.

I juni 1998 kom kommissionen med ett förslag till direktiv där framför allt marknadsperspektivet på elektroniska signaturer berörs. Medlemsstaterna uppmanades att säkerställa integritet och dataskydd samt se till att de som tillhandahåller säkerhetscertifikat har relevanta kunskaper om säkerhetsarbetet. I bilagor angavs kriterier för krav på s.k. kvalificerade certifikat och krav på tillhandahållare av certifikattjänster. I december 1999 antog Europaparlamentet och rådet direktivet med vissa förändringar. Bland annat hade man lagt till att medlemsstaterna bör garantera lämplig övervakning av tillhandahållare av certifikat samt utse lämpliga organ för att övervaka

att anordningar för skapande av signaturer överensstämmer med fastlagda kriterier. Utöver detta hade man lagt till två bilagor: Krav på säkra anordningar för skapande av signaturer samt Rekommendationer för säker signaturverifiering. I juli 2003 fastställde kommissionen tre tekniska kravdokument enligt *Common Criteria* som anger IT-säkerhetskriterier för anordningar som utställer certifikat, samt på anordningar som skapar kvalificerade elektroniska signaturer. Kommissionen har sedan återkommit till frågan om signaturer åtminstone två gånger – dels vid halvtidsöversynen av e-Europa 2005, dels vid uppdateringen av handlingsplanen för e-Europa 2005.

Smarta kort nämndes i e-Europa 2002 som ett instrument för att uppnå en ökad säkerhet. I april 2000 publicerades också en Smart Card Charter, inklusive vad som kallades Smart Card Action Plan inom ramen för e-Europa 2002. Dessa ingick i ett initiativ kallat e-Europa Smart Cards (eECC) som drevs gemensamt av producenter och utgivare av smarta kort, men där också kommissionen var en finansiär och intressent. Inom ramen för initiativet producerades ett dokument kallat Common Requirements och genomfördes så kallade vägbrytande verksamheter. Initiativet synes ha avslutats och möjligen kan intresset för smarta kort ha minskat. Någon referens till smarta kort har inte gått att finna i till exempel halvtidsöversikten av e-Europa 2005.

Kampen mot IT-brottslighet

I utredningens andra delbetänkande redogjordes för det rambeslut om angrepp mot informationssystem, som då ännu inte formellt antagits av rådet. Rambeslutet, som antogs av rådet den 24 februari, 2005, syftar till att tillnärma medlemsstaternas straffrättsliga lagstiftning när det gäller angrepp mot informationssystem och därigenom förbättra samarbetet mellan rättsliga och andra myndigheter. Rambeslutet innehåller bestämmelser om definitioner, olagligt intrång i informationssystem, olaglig systemstörning, olaglig datastörning, anstiftan, medhjälp och försök, påföljder och försvårande omständigheter, ansvar och påföljder för juridiska personer, behörighet samt utbyte av personuppgifter. En promemoria som behandlar de lagändringar som krävs i Sverige med anledning av rambeslutet remissbehandlas för närvarande (Ds 2005:5 EU:s rambeslut om angrepp mot informationssystem). I promemorian konstateras att straffansvaret måste utvidgas för att Sverige skall leva upp till de

krav som ställs i rambeslutet. Det gäller att kriminalisera fall där en upptagning för databehandling görs obrukbar, undanskaffas eller förstörs, eller där användningen av en sådan upptagning hindras eller uppgifterna görs oåtkomliga. Kriminaliseringen innebär till exempel att så kallade tillgänglighetsattacker blir straffbara. Promemorian har remissbehandlats.

Ytterligare ett rambeslut som har särskild bäring på IT-brottslighet är för närvarande föremål för förhandling inom EU. Rambeslutet rör lagring av Internet- och teletrafikuppgifter för brottsbekämpningsändamål och initiativet kommer ursprungligen från fyra medlemsstater, bland dem Sverige. Bakgrunden till förslaget är terroristattentaten i Madrid, vilka föranledde EU:s stats- och regeringschefer att anta en deklaration i kampen mot terrorism i vilken man bland annat uppmanade medlemsstaterna att med prioritet behandla ett förslag om lagring av Internet- och teletrafikuppgifter. Rambeslutet är i dess nuvarande formulering inte begränsat till att gälla enbart kampen mot terrorism. Syftet är att uppgifter om Internet- och teletrafik, i korthet uppgifter om vilka datorer eller telefoner som stått i förbindelse med varandra vid en viss tidpunkt, skall bevaras för att de brottsbekämpande myndigheterna skall kunna få tillgång till uppgifterna i utredningen av brott. För bekämpningen av den IT-relaterade brottsligheten, till exempel de brott som harmoniseras genom rambeslutet om angrepp mot informationssystem, skulle en sådan ordning underlätta spårande av ursprunget till exempelvis ett intrång eller ett intrångsförsök.

5.3 Samverkan inom internationella organisationer

Europarådets IT-brottskonvention kommenterades kort i utredningens andra betänkande. Konventionen, som förhandlades fram i slutet av 1990-talet och antogs 2001, företer likheter med det inom EU antagna rambeslutet om angrepp mot informationssystem, och var också en föregångare till det senare. Konventionen och rambeslutet har definitioner som i allt väsentligt motsvarar varandra. Vidare föreskrivs om kriminalisering av vissa gärningar i båda instrumenten. Reglerna om ansvar och påföljder för juridiska personer och om jurisdiktion är också i stort sett lika i konventionen och rambeslutet. Några huvudsakliga skillnader finns dock. I rambeslutet har man i viss mån gått längre än konventionen genom att

föreskriva om påföljder och reglera försvårande omständigheter, medan konventionen å andra sidan kriminaliserar fler gärningar än rambeslutet, till exempel dataförfalskning och databedrägeri. Konventionen innehåller även processrättsliga regler för säkrande av bevisning. Ett exempel är åtagandet att införa regler om skyndsamt säkrande av bevisning i elektronisk form. Till konventionen har utarbetats ett tilläggsprotokoll som behandlar frågan om ansvar för och utredning av gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av datorsystem.

För utredningens del är konventionen främst av intresse för de hjälpmedel den skapar för utredningen av IT-brott så som angrepp mot informationssystem. Dylika brott har inte sällan en internationell koppling, som medför att det internationella samarbetet blir avgörande för en framgångsrik brottsutredning. En styrka hos konventionen i förhållande till rambeslutet är att den omfattar fler länder. Såväl USA som Japan och Kanada deltog i utarbetandet av konventionen och har möjlighet att ansluta sig densamma. För utredningen av IT-brott med internationella förgreningar är det förstås av stor betydelse med ett instrument som en så stor del av världens IT-nationer kunnat enas om. Konventionen trädde i kraft den 1 juli 2004 och hade den 1 maj 2005 undertecknats av 42 stater. Ratificering hade vid samma tidpunkt skett i tio stater, men i flertalet medlemsstater inom Europarådet som undertecknat konventionen pågår arbete med att genomföra denna. I Sverige har promemorian Ds 2005:6 Brott och brottsutredning i IT-miljö utarbetats och är för närvarande föremål för remissbehandling. I promemorian föreslås de lagändringar som krävs för att Sverige skall kunna ratificera konventionen och dess tilläggsprotokoll.

5.4 OECD:s riktlinjer för nät- och informationssäkerhet

I utredningens uppdrag ingår att beakta OECD:s riktlinjer och lämna förslag till hur riktlinjerna kan implementeras i Sverige. Riktlinjerna har därför utgjort en av utgångspunkterna för utredningsarbetet, vilket också redovisats i avsnitt 2.

OECD:s riktlinjer för nät- och informationssäkerhet har som mål att

– främja en säkerhetskultur bland alla deltagare *(användare)* som ett sätt att skydda informationssystem och nät,

- göra deltagarna *(användarna)* medvetna om riskerna för informationssystem och nät, om de regler, förfaranden, åtgärder och rutiner som står till buds för att ta itu med dessa risker och om nödvändigheten att införa och tillämpa dessa,
- främja ett ökat förtroende hos alla deltagare *(användare)* för informationssystem och nät och för det sätt på vilket de tillhandahålls och används,
- skapa en allmän referensram som hjälper deltagarna *(användarna)* att förstå säkerhetsfrågorna och ta hänsyn till etiska värderingar vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner för säkerheten i informationssystem och nät,
- uppmuntra alla deltagare *(användare)* att samarbeta och utbyta relevant information vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner som rör säkerheten,
- arbeta för att alla som deltar vid utveckling och införande av standarder skall uppfatta säkerhet som ett viktigt mål.

Målsättningarna med OECD:s riktlinjer är enligt utredningens mening rimliga och kan bidra till en gemensam inriktning av informationssäkerhetsarbetet på nationell nivå och kan underlätta Sveriges samverkan med andra länder. Tillsammans med utredningsförslagen är riktlinjerna en bra utgångspunkt för en gemensam lägsta nivå för informationssäkerhetsarbetet. De är intuitivt formulerade vilket torde öka möjligheterna till efterlevnad. Å andra sidan kan riktlinjerna anses väl generella och inte tillräckliga med avseende på konkret innehåll. Flera aktörer torde redan i dag, utan formella krav att följa riktlinjerna, kunna säga sig ha uppfyllt dem. Det är möjligt att en uppstramning av riktlinjerna skulle öka möjligheterna till att skapa en gemensam grund för att informationssäkerhetsarbetet uppfylls.

Mot denna bakgrund lämnar utredningen förslag i frågor som rör medvetenhet, ansvar och förutsättningar för ökad delaktighet och fördjupad demokrati. Genom förslagen till ökade krav på säkerhet vid elektronisk kommunikation och bred samverkan mellan alla aktörer läggs grunden för en dialog som även kan öka medvetenheten om de etiska aspekter, som bör läggas. Utredningen föreslår vidare att såväl det privata som det offentliga åtagandet måste omfatta ett ansvar för informationssäkerheten i den egna verksamheten. Frågor som rör hantering av riskbedömningar, utformning och genomförande av säkerhetsåtgärder, säkerhetshan-

teringen samt ansvaret för fortlöpande omprövning kommer därmed att följa ansvarsprincipen. Utredningen visar även på möjligheter att författningsmässigt upprätthålla grundläggande säkerhet i samhällsviktig verksamhet. Slutligen pekar utredningen på vikten av att staten måste ha en förmåga till omedelbar reaktion för att förhindra, upptäcka och reagera på incidenter.

Utredningen anser mot denna bakgrund att de olika utredningsförslagen innebär ett genomförande av OECD:s riktlinjer i Sverige. Det måste dock än en gång framhållas att OECD:s riktlinjer endast är allmänt hållna och kan uppfyllas med olika ambitionsnivå. Det är därför, enligt utredningens mening, nödvändigt att ytterligare fördjupa och konkretisera vilka åtgärder som skall prioriteras i det fortsatta arbetet.

5.5 Utredningens slutsatser rörande den internationella dimensionen

Utredningen har valt att inledningsvis betona de europeiska och de internationella sammanhangen. Informationssäkerhet är ett gemensamt, internationellt problem och de strategiska lösningarna måste därför utvecklas i samverkan med andra länder, både inom EU och i internationella organ.

Utredningen gjorde i sitt andra delbetänkande en översiktlig redogörelse för det arbete som har bedrivits inom EU på informationssäkerhetsområdet de senaste åren. Utredningen kan konstatera att sedan publicerandet av det delbetänkandet har arbetet med informationssäkerhet gått framåt inom flera olika områden. Sedan i mars 2004 finns Europeiska nät- och informationssäkerhetsbyrån (Enisa) som behandlar informationssäkerhetsfrågor (se avsnitt 5.2). På integritetsområdet diskuteras frågan om uppgiftsskyddsombud och deras uppgifter. Kommissionen har vid ett flertal tillfällen återkommit till frågan om elektroniska signaturer, bland annat vid halvtidsöversynen av e-Europa 2005 och vid uppdateringen av handlingsplanen för samma projekt. I kampen mot IT-brottsligheten har rådet antagit ett rambeslut med syftet att tillnärma medlemsstaternas strafflagstiftning när det gäller angrepp mot informationssystem. Samtidigt förhandlas ett rambeslut som syftar till att tillse att uppgifter om Internet- och teletrafik – vilka uppkopplingar som stått i förbindelse med varandra vid en viss

tidpunkt – bevaras under en viss tid för att finnas tillgängliga för brottsbekämpande myndigheter vid utredningar av brott.

Utredningen konstaterade redan i sitt andra delbetänkande att internationellt utbyte på informationssäkerhetsområdet från svenskt håll har varit splittrat och inte i tillräcklig utsträckning samordnat på nationell nivå. Det gäller inte bara bevakning av positioner och åtaganden utan även genom bristande bearbetning och delgivning av inhämtad information i olika sammanhang. För att Sverige skall ha fortsatt gott genomslag inom området måste även det internationella utbytet samordnas, precis som svenska ställningstaganden i policyfrågor. Utredningen avser att återkomma till dessa frågor i slutbetänkandet.

OECD antog 2002 riktlinjer för säkerheten i nät- och informationssystem. Målsättningarna med riktlinjerna är enligt utredningens mening rimliga och kan bidra till en gemensam inriktning av informationssäkerhetsarbetet på nationell nivå och kan underlätta Sveriges samverkan med andra länder. Utredningen anser att de förslag som utredningen presenterar innebär ett genomförande av OECD:s riktlinjer i Sverige. Det måste dock framhållas att OECD:s riktlinjer endast är allmänt hållna och kan uppfyllas med olika ambitionsnivå. Det är därför, enligt utredningens mening, nödvändigt att ytterligare fördjupa och konkretisera vilka åtgärder som skall prioriteras i det fortsatta arbetet.

6 Gränser för det offentliga åtagandet

Informations- och kommunikationstekniken har möjliggjort en explosionsartad utveckling inom informationsförsörjningen. Sverige innehar en framstående ställning internationellt i fråga om användning av ny teknik. De investeringar i människor, kompetens och teknik som redan är genomförda utgör en värdefull potential för framtiden och måste kunna vara en utgångspunkt för kommande informationssäkerhetsarbete. En för utredningen central tanke har varit att söka finna metoder och modeller att ta tillvara den samlade kapaciteten genom en bättre utvecklad samverkan och en tydligare arbetsfördelning mellan olika aktörer i samhället. Ökad informationssäkerhet handlar därför enligt utredningens synsätt inte i första hand om ytterligare investeringar utan snarare om en tydligare ansvars- och arbetsfördelning mellan olika aktörer – vad skall ligga inom respektive verksamhetsansvariges åtagande respektive var skall gränsen gå för det offentliga åtagandet på informationssäkerhetsområdet?

Den gemensamma strategin, som utredningen redovisar, är därvid en viktig förutsättning för att kunna utveckla formerna för samverkan och arbetsformer. Vidare krävs ett regelverk som stödjer, tydliggör eller framtvingar krav på aktörer och som säkerställer att informationssäkerheten efterlevs.

Informationssäkerhetsproblematiken skär genom samhällets alla delar och nivåer, från statlig nivå till den enskilde individen med dator i hemmet. Privat och offentlig sektor är del av, och drabbade av, samma informationssäkerhetsproblematik och båda sektorerna kan också bidra till att förbättra situationen på olika sätt. Förutsättningarna och behoven skiftar och samverkan mellan de båda sektorerna är nödvändig.

Det är viktigt att notera att flera olika samarbetskonstellationer, såväl nätverk som samverkansgrupper, redan finns inom både privat

och offentlig sektor. Det kan dock ligga ett värde i att se över behoven av samverkan och effektivisera de fora som finns.

Problemet är snarast att få så många olika aktörer och aspekter på informationssäkerhet som möjligt att samverka i en given riktning. Frågeställningen handlar inledningsvis om säkerheten på samhällsnivå och omfattar alla aktörer. Problemställningarna ser emellertid olika ut beroende på om man betraktar relationer mellan medborgare och företag, mellan medborgare och den offentliga sektorn eller mellan företag och staten. En annan sida av samma frågeställning handlar om samverkan inom respektive grupper av aktörer. Vad faller inom medborgarens eget ansvar respektive under företagens ansvar? Vilka problemställningar inryms i samverkan mellan stat och kommun eller mellan grupper av myndigheter?

6.1 Utvecklingen leds av marknaden

Den tekniska utvecklingen på IT-området är i allt väsentligt styrd av olika privata aktörer på marknaden. Tekniska framsteg omsätts mycket snabbt i olika applikationer. På motsvarande sätt expanderar marknaden för informationssäkerhet och omfattar allt mer av såväl offentlig som privat verksamhet. Det betyder att allt fler verksamhetsprocesser stöds av system för elektronisk hantering av data och tillverkarnas produkter och system styrs av programvaror och blir i allt högre grad uppkopplingsbara över kommunikationsnät för styrning, övervakning, service och så vidare. Därmed kommer allt större krav att ställas på den gemensamma infrastrukturen vad gäller leveranssäkerhet och kvalitet.

Den tekniska utvecklingen skapar nya möjligheter och därmed nya säkerhetsproblem. En rimlig slutsats är därför att de aktörer som skapar de nya möjligheterna också borde vara bäst på att lösa de säkerhetsproblem som uppstår. Eftersom utvecklingen huvudsakligen finns i marknaden är det också i första hand där som säkerhetslösningarna måste utvecklas.

Ett av problemen är dock att det inte alltid finns en efterfrågan på säkerhetslösningar som genererar en fungerade marknad. Detta är särskilt bekymmersamt inom vissa samhällsviktiga verksamheter, där verksamhetsutbudet/den potentiella marknaden är starkt begränsad eller obefintlig. Den drivande kraften bakom utveckling av informationssäkerhet måste därför i dessa fall sökas på den offentliga

sidan, hos respektive sektorsansvariga myndigheter. Dessa svarar för tillämpning av regler och bestämmelser, för tillsyn och har ofta rollen av kravställare gentemot de privata aktörer som verkar inom sektorn. Ett exempel på detta är det finansiella området, där Finansinspektionen i samverkan med branschen utvecklar informationssäkerheten som en integrerad del av säkerheten i den samlade verksamheten. Ett annat exempel är FDA (Food and Drug Administration) i USA, där av FDA utfärdade detaljkrav på uppföljning av varje steg i tillverkningsprocessen och i utveckling av nya läkemedel har kommit att styra stora delar av läkemedelssektorns sätt att utveckla, bygga och driva administrativa IT-tillämpningar. IT-branschen ställs då inför utmaningen att kunna leverera lösningar som svarar mot FDA:s krav, vilket tvingar fram lösningar och stimulerar utvecklingen.

Ett exempel på betydelsen av statens roll som kravställare och aktör för ökad tillgänglighet av certifierade IT-säkerhetsprodukter är USAs beslut NSTISSC No. 11 från juli 2003. Beslutet innebär att samtliga produkter som ska upphandlas till statliga myndigheter, som innehåller IT-säkerhetsfunktioner och som hanterar information som rör nationell säkerhet, måste vara evaluerade och certifierade i enlighet med *Common Criteria*, av NIST eller av NSA. Inom ett år ökade antalet pågående certifieringar av IT-säkerhetsprodukter i den amerikanska certifieringsordningen för *Common Criteria* med mer än 400%, från 30 (2003) till 130 (2004). Beslutet har lett till att USA i dag är den överlägset ledande nationen när det gäller att utveckla IT-säkerhetsprodukter certifierade enligt *Common Criteria*. På sikt kan detta komma att både gynna amerikansk export av IT-säkerhetsprodukter och bidra till ökat skydd av den egna infrastrukturen.

Enligt utredningens mening bör dessa synsätt ligga till grund för samverkan mellan privat och offentlig verksamhet. Det innebär att staten i första hand bör utnyttja sin olika roll som kravställare på säkerhet i olika verksamheter i stället för att genom olika regulatoriska åtgärder försöka precisera tekniska krav på informations- och kommunikationssystem.

6.2 Förutsättningar för privat-offentlig samverkan

Som utredningen tidigare redovisat är skillnaderna mellan privat och offentlig sektor stora med avseende på struktur, organisation

och representativitet. Staten kan därför inte överföra de modeller och metoder som tillämpas för samverkan inom offentlig sektor. Staten kan heller inte förvänta sig att marknadens aktörer skall ta till sig och utveckla samverkansformer som liknar statens interna modeller.

Företrädare för näringslivet har framhållit flera exempel på en väl fungerande samverkan inom områden där staten har ett avgörande inflytande. Inom bankväsendet pågår sedan lång tid tillbaka ett konstruktivt samarbete i informationssäkerhetsfrågor som en del av säkerheten och förtroendet för den finansiella sektorn. Det behöver således inte råda någon motsättning mellan statens respektive näringslivets intressen, inte ens på starkt reglerade områden. Med denna förebild har utredningen vid flera tillfällen kunnat konstatera att olika representanter för näringslivet välkomnar en bredare samverkan kring informationssäkerhet till ömsesidig nytta men att samverkan måste vila på frivillighet. Enligt utredningens mening borde det vara möjligt att inom ytterligare sektorer utveckla samverkan i syfte att öka informationssäkerheten, särskilt om uppgiften att förebygga och förbereda tydliggörs för ytterligare myndigheter med sektorsansvar som involverar näringslivet som aktörer. Av dessa aktuella myndigheter ingår sannolikt flera i KBM:s samverkansområden och några disponerar dessutom vissa medel inom den så kallade civila ramen för åtgärder som rör den fredstida krishanteringsförmågan. Om dessa myndigheter skulle kunna disponera dessa medel även för sådana informationssäkerhetsåtgärder som stärker samhällets samlade säkerhet skulle det sannolikt bidra till en mer utvecklad samverkan.

Ovanstående resonemang är exempel på hur informationssäkerhet, som en integrerad del i respektive verksamhet, skulle kunna hanteras i samverkan. Den tvärsektoriella aspekten av informationssäkerhet kan däremot inte hanteras på samma sätt då det bland annat handlar om behov av att lösa vissa gemensamma frågor eller att formulera grundläggande krav eller att författningsreglera. Det finns också behov av att fortlöpande belysa vilka faktiska hot och risker som finns på informationssäkerhetsområdet, så att dessa kan beaktas och anpassas till respektive verksamhets förutsättningar. På dessa områden har staten internationella kontaktytor, överblick och möjligheter till underrättelseinhämtning som de flesta företag saknar. I dessa tvärsektoriella frågor finns dock inget entydigt gränssnitt eller kontaktpunkt

mellan stat och näringsliv. Staten måste således hitta former för en dialog med näringslivet som får anpassas till varierande förutsättningar. Det staten kan göra handlar då om att tydliggöra sin egen uppgift och att utdela ansvar till en myndighet med sammanhållande ansvar.

6.3 Samverkan inom offentlig sektor

Utredningen har tidigare konstaterat att staten har i stort sett samma problembild att hantera som Sveriges Kommuner och Landsting. Det handlar om gränssnittet mellan myndigheter och medborgare, om tillit och förtroende och möjligheter till ökad delaktighet i den offentliga verksamheten och om ökad tillgänglighet till information med bevarad integritet och trygghet. En utveckling av informationsförsörjning i alla dessa avseenden förutsätter att ett antal säkerhetsproblem löses. Vidare har staten och kommunerna en i allt väsentligt likartad struktur, både politiskt och organisatoriskt. Förutsättningarna för samverkan inom staten respektive mellan kommuner företer således många likheter.

Kommunerna uppvisar dock stora inbördes skillnader i fråga om storlek, förutsättningar, behov och system. Detta hindrar dock inte att samverkan skulle kunna utvecklas i fråga om vilka grundläggande krav på informationssäkerhet som bör eftersträvas i relation till medborgare och företag, vilka krav på integritet och trygghet som bör eftersträvas samt vilka krav på tillgänglighet som bör upprätthållas – allt i syfte att skapa så likartade och rättvisande förutsättningar som möjligt över hela landet. Det kan även finnas anledning att samverka i frågor som rör medvetandegörande, kompetensförsörjning etc. I en sådan samverkan är det enligt utredningens mening viktigt att staten, liksom i relation till näringslivet, i möjligaste mån, begränsar sin roll till beställarens/kravställarens och överlämnar genomförandet/tillämpning till den det berör, det vill säga den enskilda kommunen. Som goda exempel på denna typ av samverkan har framförts den modell som tillämpats vid bredbandsutbyggnaden.

Inom området civilt försvar har funnits en överenskommelse mellan regeringen och Svenska Kommunförbundet som skulle kunna tjäna som förebild. Kommunerna erhåller i dag en årlig ersättning från den civila ramen för sina uppgifter på området. Det

kan enligt utredningen finnas skäl att genom en särskild överenskommelse bekräfta en samsyn i informationssäkerhetsfrågor och att tydliggöra att kommunerna kan disponera tillgängliga statliga medel även för dessa ändamål. I detta sammanhang kan ett gemensamt kommunikationsnät diskuteras, såsom har beskrivits i kapitel 4.

6.4 Det privata åtagandet

Varje enskild verksamhetsansvarig ansvarar själv för säkerheten och funktionaliteten i sin verksamhet. Informationssäkerhet, såväl teknisk som administrativ, måste ses som en integrerad del av verksamhetsansvaret och skiljer sig på så vis inte nämnvärt från andra typer av säkerhetsrisker. Åtagandet skulle således följa ansvarsprincipen.

Enligt utredningens mening måste det ligga inom varje medborgares eget ansvar att inhämta kunskaper och vara medveten om de säkerhetsrisker som följer med elektronisk hantering. Det är vidare rimligt att begära att varje datoranvändare utnyttjar något av de programmässiga och tekniska hjälpmedel som finns att tillgå på marknaden. Utredningen konstaterar samtidigt att utbudet av nyckelfärdiga lösningar för en vardagsanvändare är begränsat, men vill inte utesluta att marknaden kommer att svara upp mot en efterfrågan på ”säkra” datorer. Enligt utredningens mening finns det ännu inte anledning att aktualisera frågor om någon form av produktkrav eller grundsäkerhetskrav av den typ som finns på elområdet. I det privata åtagandet bör således ansvaret för den egna datorsäkerheten inkluderas. Kravet på säker kommunikation är dock en helt annan fråga, där staten har anledning att agera för den enskilde medborgarens säkerhet.

På motsvarande sätt anser utredningen att det i princip måste ligga inom varje företags åtagande att svara för såväl kompetensförsörjning som säkerheten i de egna informationssystemen. I det privata åtagandet måste även ingå att säkerställa säkerheten i det fall att någon utomstående anlitas för tjänster av olika slag, till exempel vid outsourcing. Det torde även finnas starka ekonomiska incitament för detta. Varje verksamhetsansvarig är skyldig att bedriva sin verksamhet inom ramen för lagar och förordningar. Informationssäkerheten är en integrerad del av verksamheten. Någon anledning att från staten sida att rikta särskilda, generella krav i dessa avseenden torde därför inte föreligga.

För samhällsviktiga verksamheter och system finns det anledning för staten att ställa särskilda krav på leveranssäkerhet, funktionalitet och kvalitet, även när verksamheten är privat eller enskild. Exempel på ett sådant utvidgat åtagande finns bland annat reglerat i lagen (2003:389) om elektronisk kommunikation (EkomL.). I det privata åtagandet kan således ingå vissa tilläggskrav som uppställs av staten.

Någonstans går dock en gräns för vad som kan inrymmas i den enskildes åtagande och vad som övergår till att involvera även staten i olika roller. Att fastställa exakt var denna gräns går är naturligtvis inte möjligt. Det grundläggande förhållningssättet bör enligt utredningen ändå vara att i det enskilda åtagandet ingår att anpassa säkerheten till den egna verksamhetens förutsättningar, funktionellt och ekonomiskt.

Det finns dock hot och risker som den enskilde medborgaren eller företagen inte kan skydda sig mot. Det kan gälla konsekvenser av mer kvalificerade hot, intrång eller antagonistiska angrepp. Men detta bör enligt utredningen inte rubba den grundläggande principen om det enskilda åtagandet. Däremot bör det i samhället finnas en förmåga att upptäcka och förhindra skadlig verksamhet, en fråga som normalt inryms i det statliga åtagandet – se vidare detta avsnitt.

6.5 Det offentliga åtagandet

Det grundläggande synsätt som utredningen redovisat på det privata åtagandet är till största del tillämpligt även på verksamheten hos myndigheter och organ inom offentlig sektor. All verksamhet skulle således innefatta ett samlat ansvar för kompetensförsörjning och säkerhet i de egna informations- och kommunikationssystemen. Även den offentliga verksamheten skall genomföras inom de ramar som ges av lagar och förordningar och informationssäkerheten bör betraktas som en integrerad del av verksamheten. Att dessa lagar och förordningar inte alltid är desamma som för enskilda verksamheter förändrar inte enligt utredningen det grundläggande förhållningssättet för det offentliga åtagandet – åtminstone inte med avseende på den egna, myndighetsspecifika verksamheten.

En helt annan fråga är att det i det offentliga åtagandet kan ingå att säkerställa vissa grundläggande samhällsfunktioner, som

rättsväsende, hälso- och sjukvård etc. I genomförandet av denna kärnverksamhet ingår i flera fall ett utvidgat åtagande för skydd av liv, egendom, miljö etc. samt att säkerställa en förmåga att hantera konsekvenser av allvarligare kriser. I dessa åtaganden kan det behövas vissa tilläggskrav på informationssäkerhet i syfte att exempelvis skydda den enskildes integritet samtidigt som krav på tillgänglighet upprätthålls eller för att kunna upprätthålla sekretess. Till statens åtagande måste också räknas vissa specialintressen och uppgifter som sammanhänger med rikets säkerhet, totalförsvaret samt underrättelse- och säkerhetstjänsterna. Med dessa åtaganden följer höga krav på förmåga att bland annat upptäcka, förhindra och hantera kvalificerade störningar eller angrepp i informations- och kommunikationssystem.

På liknande sätt bör det ingå i det offentliga åtagandet att säkerställa att samhällsviktig verksamhet och samhällsviktiga system uppfyller särskilda krav på leveranssäkerhet och kvalitet, oavsett om verksamhet bedrivs i privat eller offentlig regi.

Staten har två unika roller och åtaganden som inte kan överlåtas till någon annan aktör. Endast staten kan besluta om spelregler på marknaden i form av författningar och endast staten kan representera svenska intressen inom EU och i internationella sammanhang på statlig nivå.

Staten har slutligen en unik position genom sin överblick, kontaktyta och sina grundlagsreglerade maktmedel. Till statens åtagande bör därför räknas uppgiften att lägga en helhetssyn på informationssäkerheten, internationellt och nationellt. I detta åtagande ingår att medvetandegöra, ta initiativ och samordna insatser från flera aktörer och att svara för grundläggande kompetensförsörjning.

Statens åtagande, ansvar och intresse skulle mot denna bakgrund kunna sammanfattas enligt följande:

1. Staten har ett extra stort ansvar för att en helhetssyn etableras och appliceras på informationssäkerheten och att nationella intressen bevakas inom EU och i internationella sammanhang.
2. Staten har ansvaret för samhällets spelregler inom informationssäkerhetsområdet.
3. Staten har ett övergripande ansvar för informationssäkerheten inom ett antal politikområden. Det gäller statens kärnverksamhet som till exempel rättsväsendet eller underrättelse- och

säkerhetstjänsterna. Det gäller även ansvaret för att olika samhällsviktiga verksamheter (el, tele etc.) bedrivs med tillräcklig säkerhet oavsett vem som äger dem.

4. Staten har slutligen ett eget intresse och ansvar för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sina olika roller som ansvarig för myndighetsutövning, i sin ägarroll etc.

Vissa aspekter av dessa åtaganden är av betydelse för hur staten bör organisera sina verksamheter och resurser. Detta kommer att redovisas i utredningens slutbetänkande i september 2005.

6.6 Utredningens slutsatser om samverkan och åtaganden

Den tekniska utvecklingen skapar nya möjligheter och därmed nya säkerhetsproblem. En rimlig slutsats är därför att de aktörer som skapar de nya möjligheterna också borde vara bäst på att lösa de säkerhetsproblem som uppstår. Eftersom utvecklingen finns huvudsakligen i marknaden är det också där som säkerhetslösningarna måste utvecklas. Staten bör i första hand utnyttja sina olika roller som kravställare på säkerhet i olika verksamheter istället för att genom olika regulatoriska åtgärder försöka precisera tekniska krav på informations- och kommunikationssystem.

Enligt utredningens mening borde det vara möjligt att inom ytterligare sektorer och områden utveckla samverkan i syfte att öka informationssäkerheten, särskilt om uppgiften att förebygga och förbereda tydliggörs för ytterligare myndigheter med sektorsansvar som involverar näringslivet som aktörer. Utredningen har vid flera tillfällen kunnat konstatera att olika representanter för näringslivet välkomnar en bredare samverkan kring informationssäkerhet till ömsesidig nytta men att denna samverkan måste vila på frivillighet. Staten måste hitta former för en dialog med näringslivet som får anpassas till varierande förutsättningar. Det staten kan göra handlar då om att tydliggöra sin egen uppgift och att utdela ansvar till en myndighet med sammanhållande ansvar.

Utredningen har tidigare konstaterat att staten har i stort sett samma problembild att hantera som Sveriges Kommuner och Landsting. Förutsättningarna för samverkan inom staten respektive mellan kommuner företer också många likheter. Det kan enligt

utredningen finnas skäl att genom en särskild överenskommelse bekräfta en samsyn i informationssäkerhetsfrågor och att tydliggöra att kommunerna kan disponera tillgängliga medel även för dessa ändamål. Varje enskild verksamhetsansvarig ansvarar själv för säkerheten och funktionaliteten i sin verksamhet. Informationssäkerhet, såväl teknisk som administrativ, måste ses som en integrerad del av verksamhetsansvaret och skiljer sig på så vis inte nämnvärt från andra typer av säkerhetsfrågor. Åtagandet skulle således följa ansvarsprincipen.

Enligt utredningens mening måste det ligga inom varje medborgares eget ansvar att inhämta kunskaper och vara medveten om de säkerhetsrisker som följer med elektronisk hantering. På motsvarande sätt anser utredningen att det i princip måste ligga inom varje företags åtagande att svara för såväl kompetensförsörjning som säkerheten i de egna informationssystemen. I det privata åtagandet måste även ingå att säkerställa säkerheten i det fall att någon utomstående anlitas för tjänster av olika slag.

För samhällsviktig verksamhet och system finns det dock anledning för staten att ställa särskilda krav på leveranssäkerhet och kvalitet, även när verksamheten drivs av privat aktör.

Det grundläggande synsätt som utredningen redovisat på det privata åtagandet är till största del tillämpligt även på verksamheten hos myndigheter och organ inom offentlig sektor. All verksamhet skulle således innefatta ett samlat ansvar för kompetensförsörjning och säkerhet i de egna informations- och kommunikationssystemen.

7 Författningsfrågor

7.1 Författningar av särskilt intresse på informationssäkerhetsområdet

Säkerhetsskyddslagen (1996:627)

I dag finns lagbestämmelser om informationssäkerhet i säkerhetsskyddslagen (1996:627). Av lagens 7 § följer att säkerhetsskyddet skall förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet röjs, ändras eller förstörs (informationssäkerhet), att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning) samt att personer som inte är pålitliga från säkerhetsskyddssynpunkt deltar i verksamhet som är av betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet skall i övrigt förebygga terrorism. Av säkerhetsskyddslagens 31 § och säkerhetsskyddsförordningens (1996:633) 39–42 §§ följer att tillsynsansvaret främst åvilar Rikspolisstyrelsen och Försvarsmakten men att även ett stort antal andra myndigheter har att kontrollera säkerhetsskyddet inom sina respektive verksamhetsområden.

Lagen gäller enligt 1 § för verksamhet hos staten, kommunerna och landstingen. Den gäller också för verksamhet hos aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande och enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Vidare gäller enligt 8 § att när staten, kommuner eller landsting skall begära in anbud eller träffa avtal om upphandling, där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, skall ett säkerhetsavtal (s.k. SUA-avtal) träffas med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Lagens tillämpningsområde är alltså begränsat till verksamhet

som är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Det finns inte någon legaldefinition av begreppet rikets säkerhet. Begreppet måste tolkas utifrån lagförarbeten och praxis. Allmänt kan begreppet sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket. Angrepp mot rikets inre säkerhet kan förekomma från grupperingar utan förbindelse med främmande makt. Såväl rikets yttre som inre säkerhet kan anses vara hotad, utan att totalförsvaret berörs (prop. 1995/96:129 s. 22 f).

Enligt 9 § i lagen skall vid utformningen av informationssäkerheten behovet av skydd för automatisk informationsbehandling beaktas särskilt. Av 11 § framgår att säkerhetsprövning skall göras innan en person genom anställning eller på annat sätt deltar i verksamhet som är av betydelse för rikets säkerhet eller för skyddet mot terrorism. Prövningen skall kartlägga om personen kan antas vara lojal mot de intressen som skyddas i lagen och i övrigt pålitlig från säkerhetssynpunkt. Anställningar och annat sådant deltagande i sådan verksamhet delas in i tre olika säkerhetsklasser beroende på i vilken omfattning den berörde får del av uppgifter som är hemliga med hänsyn till rikets säkerhet. När det gäller anställningar som har placerats i säkerhetsklass skall säkerhetsprövningen även omfatta registerkontroll, det vill säga att uppgifter hämtas från olika polisregister med mera. För placering i klass 1 och 2 skall även särskild personutredning utföras. Registerkontroll kan också göras till skydd mot terrorism.

Säkerhetsskyddsförordningen (1996:633)

I säkerhetsskyddsförordningen (1996:633) finns närmare bestämmelser om säkerhetsskydd. Enligt 5 § i förordningen skall myndigheter och andra som förordningen gäller för, undersöka vilka uppgifter i deras verksamhet som skall hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) skall dokumenteras. Enligt 6 § skall det, om det inte är uppenbart obehövligt, hos myndigheter och andra som förordningen gäller för finnas en säkerhetsskyddschef som utövar kontroll över

säkerhetsskyddet. I förordningen finns också bestämmelser bl.a. om inventering och försändelse av handlingar som omfattas av sekretess och som rör rikets säkerhet (hemliga handlingar).

Av 12 § i förordningen framgår att innan en myndighet inrättar ett register, som skall föras med hjälp av automatisk databehandling och som kan förutses komma att innehålla sådana uppgifter att utlämnandet av dem var för sig eller sammanställda kan skada totalförsvaret, skall myndigheten samråda med Försvarsmakten och, om uppgifternas natur ger anledning till det, Rikspolisstyrelsen. I fråga om uppgifter av betydelse för rikets säkerhet i övrigt skall i motsvarande fall samråd ske med Rikspolisstyrelsen. Ett system, som av flera personer skall användas för automatisk informationsbehandling av hemliga uppgifter, skall vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten. Systemet får inte tas i drift förrän det från säkerhetssynpunkt har godkänts av den för vars verksamhet systemet inrättas.

Enligt 13 § samma förordning skall myndigheter och andra som förordningen gäller för, innan de sänder hemliga uppgifter i ett datanät utanför sin kontroll, förvissa sig om att det för uppgifterna finns en fullgod informationssäkerhet. Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.

Rikspolisstyrelsen, i praktiken Säkerhetspolisen, och Försvarsmakten har enligt 39 § i förordningen ansvaret för att kontrollera säkerhetsskyddet hos myndigheterna. Rikspolisstyrelsen och Försvarsmakten har vidare, med stöd av 43–44 §§ samma förordning meddelat verkställighetsföreskrifter för respektive tillsynsområde. I föreskrifterna finns bestämmelser bland annat om informationssäkerhet.

I Rikspolisstyrelsens föreskrifter och allmänna råd ges tillämpningsföreskrifter till säkerhetsskyddslagen när det gäller informationssäkerhet, tillträdesskydd och säkerhetsprövning samt förfarandet vid registerkontroll. Föreskrifterna gäller för statliga myndigheter samt för kommuner och landsting. Bestämmelserna om informationssäkerhet gäller för uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet (hemliga uppgifter).

I den omarbetade föreskrift, som trädde i kraft den 1 februari 2005, (RPSFS 2004:11, FAP 244-1) har bestämmelserna om informationssäkerhet delats upp i två delar. Ett kapitel behandlar

informationssäkerhet för hemliga handlingar i skrift eller bild och ett kapitel om informationssäkerhet för hemliga uppgifter i IT-system. Av föreskrifterna framgår bl.a. att myndighetens chef skall fastställa mål och riktlinjer för IT-säkerheten, liksom instruktioner för användning, förvaltning och drift av IT-system som används för hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. För ett sådant IT-system skall finnas en av myndighetens chef utsedd person som ansvarar för säkerheten i systemet. Föreskrifterna innehåller vidare krav på att sådana IT-system skall vara försedda med tekniska och/eller administrativa åtgärder för identifiering av användaren, verifiering av identiteten, styrning av åtkomsträttigheter samt registrering av aktiviteter (behörighetskontroll) och loggning av bland annat användaridentitet och aktiviteter av betydelse för säkerheten i systemet (säkerhetsloggning). Vidare finns bestämmelser om bland annat skydd mot skadlig kod, intrångsskydd, incidenthantering och säkerhetskopiering.

Föreskrifterna är framtagna i samarbete med andra berörda myndigheter, bl.a. Försvarsmakten, Statskontoret och Krisberedskapsmyndigheten. Föreskrifterna skiljer sig dock delvis från de föreskrifter som Försvarsmakten meddelat. En ambition vid framtagandet av föreskrifterna har varit att de inte skall stå i strid med de rekommendationer som lämnas i BITS[1] för att underlätta för de myndigheter som valt att följa dessa. Rikspolisstyrelsen ställer dock i flera avseenden högre krav.

Förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap

I förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap ställs specifika krav på myndigheter med ett särskilt ansvar för fredstida krishantering och för förmågan att fungera under höjd beredskap. Enligt 4 § i förordningen skall myndigheter som har ett särskilt ansvar för fredstida krishantering planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom sina respektive samverkansområden. De skall därvid särskilt beakta säkerhetskraven bland annat för de tekniska system som är nödvändiga för

[1] Krisberedskapsmyndigheten (KBM) utfärdade rekommendationer, förslag till basnivå för IT-säkerhet.

att de skall kunna utföra sitt arbete. Enligt 11 § samma författning skall myndigheter med s.k. bevakningsansvar ansvara för att dator- och kommunikationssystem uppfyller sådana säkerhetskrav att de kan utföra sina uppgifter på ett tillfredställande sätt även under höjd beredskap. I förordningens 22 § ges Krisberedskapsmyndigheten rätt att meddela verkställighetsföreskrifter avseende 6–12 §§ utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket.

Krisberedskapsmyndigheten har utfärdat rekommendationer, förslag till basnivå för IT-säkerhet, benämnt BITS. Dessa rekommendationer innehåller definitioner som rör de delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring detta. Definitionerna följer i huvudsak SIS tekniska rapport Handbok 550: Terminologi för informationssäkerhet (2003). De är väl förankrade såväl nationellt som internationellt. En indelning görs i administrativ respektive teknisk informationssäkerhet.

Lagen (1990:217) om skydd för samhällsviktiga anläggningar

I lagen (1990:217) om skydd för samhällsviktiga anläggningar med mera (skyddslagen) ges bestämmelser om vissa åtgärder till skydd mot sabotage, terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och spioneri samt mot röjande av hemliga uppgifter som rör totalförsvaret. Lagen ger möjlighet att begränsa tillträdet till en anläggning eller ett område genom att förklara det som skyddsobjekt. Som skyddsobjekt får förklaras bland annat anläggningar eller områden som används eller är avsedda för ledning av befolkningsskyddet och räddningstjänsten eller det civila försvaret i övrigt, för energiförsörjning, vattenförsörjning, rundradioförsörjning, radio- och telekommunikationer, transporter eller försvarsindustriella ändamål. Att ett objekt förklaras som skyddsobjekt innebär bland annat att obehöriga inte får tillträde till objektet och att den som vill ha tillträde måste uppge sin identitet och vara beredd att underkasta sig kroppsvisitation. Den som bevakar ett skyddsobjekt har särskilda befogenheter att ingripa, bland annat mot den som det finns skäl att anhålla för spioneri eller sabotage eller förberedelse till sådant brott.

I lagen definieras inte vad som är en samhällsviktig anläggning. Däremot kan det sägas följa av vad som enligt 4 § får förklaras som skyddsobjekt vad som kan anses utgöra en samhällsviktig anläggning. Enligt 3 § i lagen kan en anläggning endast förklaras som ett skyddsobjekt för de ändamål som anges i 1 § i lagen. Det måste alltså finnas ett behov av att begränsa allmänhetens tillträde eller rätt att utnyttja en anläggning, ett område m.m. med hänsyn till skyddet mot sabotage, terroristbrott med mera.

Lagen tar inte direkt sikte på säkerheten vid hanteringen av information utan på det fysiska skyddet för anläggningar som behöver skyddas för de i lagen speciellt angivna ändamålen såsom skydd mot sabotage, spionerі med mera. Lagen innehåller därför endast bestämmelser om tillträdesbegränsning och bevakning av skyddsobjekt. Bestämmelser om hur information som behandlas vid och kommuniceras in och ut från dessa skyddsobjekt skall skyddas saknas således.

Sekretesslagen (1980:100)

I 2 kap. sekretesslagen (1980:100) finns regler om sekretess med hänsyn till rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation. I 2 kap. 1 § regleras den s.k. utrikessekretessen och i 2 kap. 2 § regleras den så kallade försvarssekretessen. Denna omfattar alla de verksamheter som är av betydelse för landets samlade försvarsåtgärder, alltså inte bara rent militära företeelser utan också åtgärder med avseende på totalförsvaret i övrigt. Det är inte bara antagna skador på landets försvar i vedertagen mening som medger sekretess, utan också ett sådant röjande av uppgifter som vållar fara för rikets säkerhet på annat sätt än genom skador för de traditionella försvarsintressena. Så kan till exempel ett röjande av uppgifter om den civila säkerhetstjänsten vålla fara för rikets säkerhet trots att någon skada för försvaret inte har inträffat. Försvarssekretessen gäller inom hela det allmännas verksamhet. Denna sekretess har dock sin största betydelse hos Försvarsmakten och andra myndigheter som ägnar sig åt militär verksamhet och frågor som avser totalförsvaret. På försvarssekretessens område är meddelarfriheten kraftigt inskränkt. Skaderekvisitet för såväl utrikes- som försvarssekretessen är rakt. Detta innebär att offentlighet är huvudregel och att sekretess endast gäller om utlämnande av uppgiften kan antas leda till skada.

Kapitel 5 i sekretesslagen reglerar sekretess främst med hänsyn till intresset att förebygga och beivra brott. Av 5 kap. 1 § andra stycket samma lag framgår att sekretess bland annat gäller för uppgift som hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Enligt 5 kap. 2 § i lagen gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd med avseende på

1. byggnader eller andra anläggningar, lokaler eller inventarier,
2. tillverkning, förvaring, utlämning eller transport av pengar eller andra värdeföremål samt transport eller förvaring av vapen, ammunition, sprängämnen, klyvbart material eller radioaktivt avfall,
3. telekommunikation eller system för automatiserad behandling av information,
4. behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling,
5. den civila luftfarten eller den civila sjöfarten, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

I InfoSäkutredningens andra delrapport konstaterades att författningsarbete pågick för att bland annat tillgodose de behov Post- och telestyrelsen har för att på ett effektivt sätt kunna bedriva den incidenthanteringsfunktion som myndigheten ålagts. Det kan nu konstateras att ändringar har genomförts i sekretesslagen i detta syfte. Därvid har 5 kap. 2 § 3 sekretesslagen utvidgats till att avse inte bara telekommunikation, utan även system för automatiserad behandling av information. Efter ändringen finns nu således en möjlighet att med stöd av sekretesslagen hemlighålla uppgifter om säkerheten avseende till exempel datorprogram i IT-system eller de loggar som datorprogrammen genererar.

Enligt 5 kap. 3 § första stycket gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att:

1. underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, eller

2. göra det möjligt att kontroller om data i elektronisk form har förvanskats, om det kan antas att syftet med metoden motverkas om uppgiften röjs.

Denna paragraf möjliggör skyddande av uppgifter i allmän verksamhet som lämnar, eller kan bidra till, upplysningar om till exempel kryptering som används för att underlätta befordran eller användning av sekretessbelagda uppgifter. Bestämmelsen möjliggör även sekretessbeläggande av hemliga nycklar som används för att skapa en så kallad elektronisk signatur som skall möjliggöra kontroll av om en handling härrör från en angiven undertecknande eller om handlingens innehåll manipulerats.

Sekretesslagen innehåller bestämmelser om när sekretess skall råda för uppgift med hänsyn till exempel rikets säkerhet eller intresset av att förebygga och beivra brott. Även om det i lagen också finns en del bestämmelser som kan sägas ta sikte på hur information ur ett administrativt och tekniskt informationssäkerhetsperspektiv skall hanteras så måste lagen i allt väsentligt anses reglera när sekretess skall råda för en uppgift och inte hur informationen administrativt och tekniskt skall hanteras ur ett informationssäkerhetsperspektiv. Lagen kan därför inte sägas vara en författning som reglerar informationssäkerhet i dess bredare bemärkelse.

Personuppgiftslagen (1998:204)

Personuppgiftslagen grundar sig på Europaparlamentets och rådets direktiv 95/46/EG från den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Av 1 § i lagen framgår att lagens syfte är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Säkerhet är en viktig del av skyddet för den personliga integriteten. Den som behandlar personuppgifter med hjälp av informationsteknik måste därför skydda uppgifterna. I lagen finns bestämmelser om säkerhet vid behandling av personuppgifter. En tillfredsställande säkerhet är ett krav enligt lagen. Enligt 31 § i lagen skall den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de uppgifter som behandlas.

Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av uppgifterna, och hur pass känsliga de behandlade uppgifterna är.

Datainspektionens allmänna råd om säkerhet preciserar personuppgiftslagens krav på säkerhet vid behandling av personuppgifter.

Ansvarig för säkerheten är enligt lagen den personuppgiftsansvarige, det vill säga den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter till någon annan som då blir att betrakta som personuppgiftsbiträde. Ett sådant biträde får behandla uppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Ett skriftligt avtal som reglerar förhållandet mellan biträdet och den personuppgiftsansvarige skall upprättas. I avtalet skall säkerhetsåtgärderna vid behandlingen av personuppgifter regleras.

Förutom krav på tillfredsställande säkerhet innehåller personuppgiftslagen även andra bestämmelser som tar sikte på att skydda människor mot att deras personliga integritet kränks när uppgifterna behandlas automatiserat.

I 9 § i lagen redovisas grundläggande krav på behandlingen av personuppgifter. I paragrafen anges bl.a. att den personuppgiftsansvarige skall se till att personuppgifter behandlas bara om det är lagligt, personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed, personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att uppgifterna därefter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Vidare anges det att den personuppgiftsansvarige skall se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen. Av stadgandet framgår vidare att inte heller fler uppgifter än vad som är nödvändigt med hänsyn till ändamålet får behandlas och att alla rimliga åtgärder skall vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

I 10 § personuppgiftslagen finns regler om när behandling av personuppgifter är tillåten. Om den registrerade inte har lämnat sitt samtycke till behandlingen får personuppgifterna bara behandlas för vissa i lagen angivna syften.

I personuppgiftslagen finns särskilda restriktioner när det gäller behandling av känsliga personuppgifter, personuppgifter om lagöverträdelser och uppgift om personnummer.

Personuppgiftslagen ställer långtgående krav på att den personuppgiftsansvarige skall informera de registrerade om den behandling av personuppgifter som utförs.

Personuppgiftslagen innehåller således en mängd bestämmelser om säkerhet vid behandling av personuppgifter. Lagens syfte och därmed de olika bestämmelsernas syfte är att skydda den enskildes integritet.

Datainspektionens allmänna råd preciserar personuppgiftslagens krav på säkerhet vid behandling av personuppgifter.

Lagen (2003:389) om elektronisk kommunikation

Det är i första hand de bestämmelser som har sitt upphov i direktivet om integritet och elektronisk kommunikation som är av intresse i detta sammanhang. Direktivet har implementerats bl.a. genom bestämmelser i 6 kap. EkomL som bland annat reglerar integritetsskydd. Av 6 kap. 2 § framgår att personuppgiftslagens bestämmelser skall gälla vid tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster om inte annat följer av EkomL. Personuppgiftslagen är således subsidiärt tillämplig i de fall där EkomL inte speciellt reglerar ett visst förhållande.

Av 6 kap. 3 och 4 §§ i lagen framgår vidare att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst skall vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät skall vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna skall vara ägnade att säkerställa en säkerhetsnivå, som med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång. Om det vid tillhandhållandet av en allmänt tillgänglig elektronisk kommunikationstjänst finns särskild risk för bristande skydd av behandlade uppgifter, skall den som tillhandahåller tjänsten informera abonnenten om risken. Om den som tillhandahåller tjänsten inte är skyldig att avhjälpa risken, skall abonnenten informeras om hur och till vilken ungefärlig kostnad risken kan avhjälpas. Den säkerhet som avses är skydd mot

obehörig avlyssning och liknande integritetskränkande handlingar, det vill säga inte drifts- och funktionssäkerhet.

I 6 kap 5–10 §§ i lagen regleras behandling av trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter. Med trafikuppgift förstås uppgift som behandlas i syfte att vidarebefordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som behövs för att fakturera detta meddelande. Huvudregeln är att det åligger anmälningspliktig tillhandahållare av allmänt kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster att utplåna eller avidentifiera dessa uppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande. Uppgifter som behövs för abonnentfakturering och för betalning av samtrafik får sparas viss tid. Detsamma gäller uppgifter som rör den som samtyckt till att dessa sparas för tillhandahållande av tjänst eller marknadsföring. Ett sådant samtycke kan när som helst återkallas. Vidare får uppgifter sparas i den utsträckning trafikuppgifterna är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst (6 kap. 8 § första stycket 3). I specialmotiveringen till paragrafen (prop. 2002/03:110) anförs att detta kan inkludera sparande av trafikuppgifter för att säkerställa straff- eller civilrättslig lagföring och även utredning och lagföring av brott, förutsatt att det sker i syfte att förhindra eller avslöja en obehörig användning av nätet eller tjänsten i fråga. Uppgifterna får enligt propositionen inte sparas längre än nödvändigt för att uppnå syftet och längre än ett år bör inte godtas om det inte föreligger särskild anledning, till exempel att förundersökning inletts. Den som tillhandahåller en allmänt tillgänglig kommunikationstjänst skall informera den uppgiften rör, om vilken typ av trafikuppgifter som behandlas och hur länge uppgifterna behandlas innan samtycke inhämtas. Lokaliseringsuppgifter som inte är trafikuppgifter, till exempel uppgifter om position från satellit, som rör användare som är fysiska personer eller abonnenter får behandlas endast sedan de avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen. Även i detta fall skall information lämnas om vilka uppgifter som kommer att behandlas och syfte med mera. Samtycke kan när som helst återkallas.

I 6 kap. 15–16 §§ i lagen finns bestämmelser om abonnentförteckning och hur dessa får behandlas. En abonnent som är en fysisk person måste informeras om vilka ändamål som finns med en allmänt tillgänglig abonnentförteckning innan personuppgifter om

abonnenten får tas upp i den. Om förteckningen återfinns i elektronisk form skall abonnenten även upplysas om vilka sökmöjligheter en sådan förteckning har. Samtycke krävs från en abonnent som är fysisk person för att behandling av personuppgifter skall vara tillåten.

I 5 kap. 7 § regleras de allmänna skyldigheter som gäller för den som tillhandahåller en allmänt tillgänglig telefonitjänst. Av stadgandet p. 1 framgår att en sådan skall se till att tjänsten och det allmänna telefonnätet till fast nätanslutningspunkt uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid. Bestämmelsen syftar dels till att möjliggöra samordning av nätfunktioner m.m. för att uppnå ett öppet och sammanhållet nät, dels till att säkerställa att en grundläggande nivå av säkerhet i den fasta telefoniinfrastrukturen uppnås genom att möjliggöra att krav ställs på förebyggande åtgärder som förstärker infrastrukturen. Bestämmelsen avser endast telefonitjänst och berör således inte de som tillhandahåller nätkapacitet eller andra typer av tjänster än telefoni. Post- och telestyrelsen (PTS) som är tillsynsmyndighet enligt EkomL har möjlighet att meddela föreskrifter om på vilket sätt dessa skyldigheter skall fullgöras och om undantag från skyldigheterna.

Av 6 kap. 19 § i lagen framgår att viss verksamhet skall bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Bestämmelsen innebär att den som bedriver anpassningsskyldig verksamhet skall använda tekniska hjälpmedel som har vissa egenskaper samt vidta de personella och organisatoriska åtgärder som krävs för att hantera hjälpmedlen. I 6 kap. 22 § samma lag finns bestämmelser om skyldighet för operatörer att – under förutsättning att det är fråga om brott av viss angiven svårighetsgrad – till brottsutredande myndigheter lämna ut vissa uppgifter om abonnemang (abonnemangsuppgifter) eller andra uppgifter om ett elektroniskt meddelande (trafikuppgifter) som annars omfattas av sekretess enligt lagen. Detta förutsätter dock att operatören inte har raderat uppgifterna. För närvarande finns inte någon skyldighet att spara trafikuppgifter för de brottsutredande myndigheternas verksamhet. Beredningen för rättsväsendets utveckling (BRU) har dock i ett tilläggsdirektiv (dir. 2003:145) fått i uppgift att göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I detta ingår bland annat att utreda vilka

typer av trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndigheterna och om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna.

Som framgått av den ovan gjorda beskrivningen innehåller EkomL vissa bestämmelser om i första hand säkerhet för behandlingen av personuppgifter. Dessa bestämmelser är således inriktade på skyddet mot integritetskränkande handlingar såsom obehörig avlyssning. Därtill innehåller lagen vissa bestämmelser beträffande telefoni och säkerhet som tar sikte på drifts- och funktionssäkerhet.

Brottsbalken (1962:700)

IT används ofta som hjälpmedel vid brott och många brott begås via Internet. Som exempel där IT ofta har stor betydelse kan nämnas grova narkotikabrott, vålds- och fridsbrott, barnpornografibrott och olika former av ekonomisk brottslighet. I brottsbalken finns vissa straffbestämmelser som är av särskilt intresse när det gäller informationssäkerhet. I 4 kap. 8 § finns bestämmelser om brytande av post- och telehemlighet. I 4 kap. 9 c § finns bestämmelser om straff för den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning (dataintrång). I 9 kap. 1 § andra stycket brottsbalken finns bestämmelser om så kallat databedrägeri. Allvarliga angrepp som riktas mot egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning, förvaltning eller upprättande av allmän ordning och säkerhet kan vara att bedöma som sabotage enligt 13 kap. 4 § brottsbalken.

Lagen (1990:409) om skydd för företagshemligheter

I lagen ges ett allmänt skydd för företagsspecifik information av teknisk, kommersiell och administrativ karaktär, oavsett om den har dokumenterats eller inte. I 1 § i lagen definieras företagshemlighet som sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende. Av samma paragraf följer att med information förstås

både sådana uppgifter som har dokumenterats i någon form, inbegripet ritningar, modeller och andra liknande tekniska förebilder, och enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något särskilt sätt. Enligt 2 § i lagen gäller denna endast obehöriga angrepp på företagshemligheter. I uttrycket hemlig ligger att näringsidkaren skall ha ambitionen att behålla informationen inom den krets där den är känd och att den inte är spridd utanför en identifierbar och sluten krets. Lagen talar dock bara om röjande av informationen och begrepp som motsvarar säkerhetsskyddslagens ”ändras” eller ”förstörs” finns inte. Informationens röjande skall dessutom vara ägnat att medföra skada för näringsidkaren i konkurrenshänseende. Lagen innehåller bl.a. regler om straff för den som olovligen bereder sig tillgång till en företagshemlighet (företagsspioneri), eller anskaffar en företagshemlighet med vetskap om att den som tillhandahåller företagshemligheten har beretts sig tillgång till den genom företagsspioneri (obehörig befattning med företagshemlighet).

7.2 Utredningens bredare definition av begreppet informationssäkerhet

Som utredningen har framhållit kan information ses som en mer eller mindre viktig resurs som kan vara utsatt för både oavsiktliga och avsiktliga hot. Oavsiktliga hot kan vara händelser såsom slump eller slarv. Skydd av information är därmed en angelägenhet för alla typer av organisationer liksom för samhället i sin helhet.

Som utredningen i tidigare avsnitt anfört fattade Europeiska unionens råd den 19 mars 2001 beslut om säkerhetsbestämmelser vilka anger hur sekretessbelagd EU-information skall hanteras. Avsikten är att skydda sekretessbelagda EU-uppgifter mot spioneri och mot att de röjs utan tillstånd. Skyddet omfattar uppgifter som hanteras i nät och system för kommunikation och information mot hot som riktar sig mot uppgifternas okränkbarhet (*integrity*) och tillgänglighet (*availability*). Avsikten är också att skydda anläggningar där EU-uppgifter förvaras från sabotage och uppsåtlig skada. Säkerheten syftar också till att – efter misslyckande – kunna bedöma omfattningen och graden av den skada som åsamkats, begränsa följderna och vidta åtgärder för att avhjälpa skadan. I bestämmelserna anges att informationssäkerhet handlar om att

fastställa och tillämpa säkerhetsåtgärder för att skydda uppgifter som har bearbetats, lagrats eller överförts i kommunikations- och informationssystem eller andra elektroniska system mot oavsiktliga eller avsiktliga sekretessbrott (*confidentiality*), och förlust av okränkbarhet eller tillgänglighet.

Enligt beslutet omfattar ”sekretessbelagda EU-uppgifter” alla uppgifter och all materiel som, om de röjdes obehörigen, skulle kunna skada EU:s intressen i olika hög grad, eller en eller flera av dess medlemsstaters intressen. Med ”handlingar” avses ett antal fysiska medier (brev, rapporter etc.) och med ”materiel” avses alla handlingar samt varje slags utrustning eller vapen.

Av särskilt intresse i detta sammanhang är säkerhetsbestämmelsernas avsnitt XI, som behandlar skydd för uppgifter som hanteras i IT- och kommunikationssystem. Hot mot system och systemens sårbarhet beskrivs där enligt följande. Ett hot kan allmänt definieras som en möjlighet till oavsiktligt eller avsiktligt äventyrande av säkerheten. När det gäller system innebär ett sådant äventyrande att en eller flera av egenskaperna sekretess (*confidentiality*), okränkbarhet (*integrity*) och tillgänglighet (*availability*) går förlorade. I bestämmelserna framhålls att sekretessbelagd och icke sekretessbelagd information som hanteras i system i koncentrerad form för snabb sökning, kommunikation och användning är sårbara i många avseenden.

Mot denna bakgrund anges att huvudsyftet med säkerhetsåtgärderna är att de skall ge skydd mot obehörigt röjande av uppgifter och mot förlust av uppgifternas okränkbarhet och tillgänglighet. För att system som hanterar sekretessbelagda EU-uppgifter skall få tillräckligt säkerhetsskydd skall lämpliga normer för konventionell säkerhet specificeras tillsammans med lämpliga säkerhetsförfaranden och säkerhetstekniker som är utformade för varje system.

Vidare föreskrivs att en väl avvägd uppsättning säkerhetsåtgärder skall fastställas och genomföras så att det skapas en säker driftmiljö för systemet. Dessa åtgärder skall tillämpas på fysiska faktorer, personal, icke-tekniska förfaranden samt driftsmetoder för datorer och kommunikation.

Enligt utredningen är dessa bestämmelser modernare och återspeglar tydligare visioner för informationssäkerhetsarbetet än det svenska regelverket. EU:s säkerhetsbestämmelser omfattar i princip all verksamhet inom EU och dess medlemsstater.

Utredningen har valt en bred definition av begreppet informationssäkerhet och har därvid tagit sin utgångspunkt i de beskrivna säkerhetsbestämmelserna. Enligt dessa syftar säkerheten till att främja tillväxt, konkurrens och välfärd. I bestämmelserna talas det om uppgifter som lagras, bearbetas och överförs i elektronisk form och att säkerheten skall uppfyllas genom krav på konfidentialitet, okränkbarhet och tillgänglighet. Kravet på okränkbarhet och tillgänglighet gäller all informationshantering, oavsett om uppgifterna är hemliga eller inte. Utredningen förordar också en reglering av informationssäkerheten i Sverige med utgångspunkt i den valda bredare definitionen av begreppet informationssäkerhet.

Fråga uppstår naturligtvis hur denna breda definition av begreppet informationssäkerhet förhåller sig till nuvarande reglering på informationssäkerhetsområdet.

Som tidigare har nämnts är det i dag endast i säkerhetsskyddslagen (1996:627) som lagbestämmelser om informationssäkerhet återfinns. I lagen finns också bestämmelser om tillträdesbegränsning och säkerhetsprövning av personal. Denna lag är därför den författning som får anses vara mest heltäckande vad gäller de olika aspekterna på information och säkerhet, även om lagens tillämpningsområde är begränsat till verksamhet som har betydelse för rikets säkerhet eller för skyddet mot terrorism.

Som framgår av den ovan gjorda genomgången och jämförelsen återspeglar nuvarande reglering på informationssäkerhetsområdet inte en sådan bredare definition av informationssäkerhet som utredningen förespråkar. Enligt utredningen föreligger det därför ett klart behov av en utökad reglering på informationssäkerhetsområdet. Den naturliga utgångspunkten vid bedömningen av vilka författningsåtgärder som blir nödvändiga med anledning av utredningens förslag blir därför nuvarande säkerhetsskyddslagstiftning.

7.3 Kan tillämpningsområdet för säkerhetsskyddslagen och säkerhetsskyddsförordningen utvidgas?

Utredningens utgångspunkt är som tidigare har framgått att informationssäkerhet är en angelägenhet för hela samhället. Behovet av en tillfredställande informationssäkerhet är inte begränsat till offentliga verksamheter. Det är inte heller begränsat till verksamheter som är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Behovet av en tillfredsställande informa-

tionssäkerhet gör sig gällande även vid verksamheter som inte har denna betydelse till exempel verksamheter innefattande kritisk infrastruktur av olika slag. Detsamma gäller verksamheter inom näringslivet. Enligt utredningen bör informationssäkerheten inte endast syfta till att skydda verksamheter av betydelse för rikets säkerhet eller skydda dem mot terrorism. Informationssäkerheten måste på samma sätt som EU:s säkerhetsbestämmelser ha det bredare syftet att också främja tillväxt, konkurrens och välfärd.

Enligt utredningen är således informationssäkerhet en fråga för hela samhället och det är motiverat med ett offentligt engagemang beträffande denna säkerhet. Engagemanget bör bland annat bestå i att det offentliga utövar en aktiv tillsyn över efterlevnaden av gällande bestämmelser inom området och genom att grundläggande säkerhetskrav ges lagstöd och preciseras i föreskrifter.

I dag utgör alltså säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) det mest heltäckande regelverket avseende informationssäkerhet. Det är som tidigare har nämnts endast i säkerhetsskyddslagen som lagbestämmelser om informationssäkerhet finns. Med stöd av säkerhetsskyddslagen och -förordningen har Försvarsmakten och Rikspolisstyrelsen meddelat föreskrifter på området. Övriga regelverk av betydelse på informationssäkerhetsområdet innehåller endast delvis bestämmelser om informationssäkerhet. Bestämmelserna är dessutom allmänt hållna.

Som tidigare nämnts är lagens tillämpningsområde dock begränsat till verksamhet som har betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Utanför lagens tillämpningområde faller därför en mängd informationshantering på vilken säkerhetskrav bör ställas för att det syfte som utredningen anser informationssäkerheten skall ha skall kunna uppnås. Som exempel kan nämnas informationshantering kring det vi kallar kritisk infrastruktur i de fall den aktuella verksamheten inte är av betydelse för rikets säkerhet. Ytterligare exempel kan vara informationshantering i verksamhet, som i sig inte är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism, men som kan vara av stor betydelse för till exempel landets handelsförbindelser och därmed för samhällets välfärd. Utredningen anser helt enkelt att det behov av säkerhet för information som tillgodoses genom nu gällande säkerhetsskyddslagstiftning i många fall gör sig lika starkt gällande även för annan samhällsviktig verksamhet än sådan som är av betydelse för rikets säkerhet eller skyddet mot terrorism.

En tanke som har förts fram är att tillämpningsområdet för säkerhetsskyddslagen skulle utvidgas till att omfatta även verksamheter som i dag inte anses vara av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism, men där informationssäkerhetsbehovet som beskrivits ovan är lika starkt. En utvidgning av tillämpningsområdet skulle kunna nås genom att begreppet rikets säkerhet gavs en annan definition än vad som är fallet i dag. Det skulle kunna rymma även de vidare aspekter som borde ingå i ett begrepp för nationell säkerhet. Det skulle kunna innefatta till exempel ekonomisk säkerhet och attraktionskraft samt handelsstatus. Begreppet rikets säkerhet används dock på olika håll i lagstiftningen bland annat i brottsbalken (1962:700) och sekretesslagen (1980:100). En ändring av begreppets innebörd skulle därför få långtgående konsekvenser och, som utredningen pekat på, bland annat påverka det straffbara området för till exempel spioneribrott.

En annan tanke skulle kunna vara att tillämpningsområdet utvidgas utan att begreppet rikets säkerhet ges en annan innebörd. En sådan utvidgning skulle få ske genom att de i lagen skyddsvärda verksamheterna och den informationshantering som där sker kompletteras med de verksamheter och den informationshantering som i dag faller utanför tillämpningsområdet men där informationssäkerhetsbehovet är stort.

En utvidgning av säkerhetsskyddslagens och därmed förordningens tillämpningsområde är förknippad med flera svårigheter. För det första är ett skäl till att bestämmelserna i lagen har den innebörd de har det faktum att de är begränsade till rikets säkerhet och terrorism. För sådan verksamhet är mer långtgående reglering beträffande säkerhet nämligen möjlig. Detta har att göra med att det för sådana verksamheter är möjligt att göra undantag från de grundläggande friheter som garanteras en enskild i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. För andra verksamheter är undantag från nämnda konvention på ett helt annat sätt begränsade. Ett utvidgat tillämpningsområde för lagen skulle därför innebära att bestämmelserna i den måste differentieras beroende på i vilken verksamhet viss informationshantering sker. Vissa bestämmelser om till exempel informationssäkerhet skulle endast komma att kunna äga giltighet vid verksamhet som är av betydelse för rikets säkerhet eller skyddet mot terrorism. För andra verksamheter skulle mindre långtgående bestämmelser om säkerhetskrav i många fall få gälla. Tydligast skulle skillnaden bli beträffande de bestämmelser som

reglerar förhållanden där integritetsskyddsaspekten gör sig starkt gällande. Detta gäller inte minst säkerhetsskyddslagens och säkerhetsskyddsförordningens bestämmelser om säkerhetsprövning och registerkontroll.

Vid ett utvidgat tillämpningsområde reses också frågan om tillsyn och tillsynsmyndighet. I dag är Rikspolisstyrelsen och Försvarsmakten tillsynsmyndigheter. Tillämpningsområdet för säkerhetsskyddslagen korresponderar med de mandat som dessa myndigheter har getts av statsmakterna. Med en utvidgning av tillämpningsområdet reses därför frågan om ytterligare en eller flera tillsynsmyndigheter. Varje myndighet har dessutom ansvar för respektive verksamhetsområde.

Ett sätt att åstadkomma ett sammanhållet regelverk på informationssäkerhetsområdet som återspeglar den bredare definition av begreppet informationssäkerhet som utredningen förordar kan således vara att utvidga tillämpningsområdet för säkerhetsskyddslagen. Sådan samhällsviktig verksamhet som inte anses vara av betydelse för rikets säkerhet eller skyddet mot terrorism, till exempel viss kritisk infrastruktur, och därmed i dag inte omfattas av säkerhetsskyddslagen skulle genom beskriven utvidgning, komma att omfattas av lagen.

En ändring av säkerhetsskyddslagstiftningen på sätt beskrivits skulle på många sätt också vara den naturliga vägen att nå ett heltäckande och sammanhållet regelverk på informationssäkerhetsområdet. Som utredningen tidigare har framhållit får redan i dag säkerhetsskyddslagstiftningen anses utgöra det mest heltäckande regelverket på området. Därtill kommer att detta regelverk vad gäller tillämpning får anses vara ett väl inarbetat.

7.4 En helt ny lag?

Ett annat sätt än att genom ändring av nuvarande säkerhetsskyddslagstiftning tillgodose utredningens bredare definition av informationssäkerhet skulle kunna vara en helt ny författning på informationssäkerhetsområdet. En sådan författning skulle kunna utgöra ett sammanhållet och mer heltäckande regelverk för informationssäkerheten i hela samhället och därmed kunna svara mot det behov som utredningen pekat på i detta avseende.

I en sådan författning skulle grundläggande bestämmelser om informationssäkerhet kunna meddelas oavsett verksamhet och slag

av informationshantering. Bestämmelserna skulle äga tillämpning oavsett om sekretess föreligger eller inte och oavsett om behandlingen avser personuppgifter eller inte och så vidare. Genom författningen skulle den bredare definition av informationssäkerhet som utredningen valt att utgå ifrån kunna omsättas i ett mera heltäckande och sammanhållet regelverk.

Tillämpningsområdet för en sådan författning bör enligt utredningen begränsas till att avse sådan samhällsviktig verksamhet som beskrivits i tidigare avsnitt. Det är för sådan verksamhet som det finns särskild anledning för staten att skapa en fastare grund för informationssäkerheten än den som skyddslagen utgör.

En författning av det slag som det nu talas om skulle råda bot på de begränsningar i tillämpningsområde som nuvarande regelverk och därvid främst säkerhetsskyddslagstiftningen innebär. Bestämmelserna i en ny författning skulle gälla även på till exempel områden och för verksamheter som inte omfattas av säkerhetsskyddslagen. Bestämmelserna skulle till övervägande del avse säkerheten i själva hanteringen av information. Som tidigare nämnts skulle de därför gälla oavsett vilken typ av skyddsobjekt det är frågan om och oavsett om behandlingen sker elektroniskt eller inte. Sekretesslagen, personuppgiftslagen m.fl. författningar som berör informationssäkerheten skulle naturligtvis gälla i tillämpliga delar såsom när fråga är vad som skall sekretessbeläggas eller när fråga är vad som särskilt gäller för behandling av personuppgifter.

Den nya författningen torde inte kunna utesluta, utan snarare förutsätta, särbestämmelser i andra författningar om informationssäkerhet på vissa områden och verksamheter till exempel beträffande informationshantering i verksamhet som är av betydelse för rikets säkerhet eller skyddet mot terrorism.

Även om en ny författning i huvudsak skulle avse säkerheten beträffande själva hanteringen av uppgifter måste enligt utredningen, för att författningen skall kunna utgöra det heltäckande regelverk på informationssäkerhetsområdet som det finns behov av, författningen även rymma regler om begränsningar i tillträde och säkerhetsprövning med registerkontroll. En sådan ny författning som nu beskrivs kräver enligt utredningen lagform.

7.5 Ett sammanhållet och heltäckande regelverk på informationssäkerhetsområdet

Framtagandet av författningsförslag med det innehåll som beskrivits ovan måste föregås av omfattande och djup analys. Detta gäller oavsett om ett sådant författningsförslag skulle avse ändringar i nuvarande säkerhetsskyddslagstiftning eller om det skulle avse en helt ny lag på informationssäkerhetsområdet. Detta gäller inte minst frågan om hur ett kraftigt förändrat eller ett helt nytt regelverk närmare skall förhålla sig till övriga författningar. En mängd följdändringar i andra författningar blir enligt utredningens bedömning också nödvändiga. Därtill kommer att det i arbetet med framtagandet av ett nytt regelverk är nödvändigt med samordning och avstämning med de tidigare nämnda övriga utredningar som pågår på informationssäkerhetsområdet. Frågan om hur ett nytt regelverk lämpligast kan åstadkommas och de närmare förutsättningarna för framtagandet av ett sådant författningsförslag måste enligt utredningen därför utredas i särskild ordning.

7.6 Steg på vägen i avvaktan på ett heltäckande och sammanhållet regelverk

Som utredningen har kunnat konstatera saknas i dag det sammanhållna och mera heltäckande regelverk om informationssäkerhet som det finns ett så stort behov av. Utredningen har med styrka framhållit att denna avsaknad och de begränsningar som följer med nuvarande regelverk innebär att ett effektivt informationssäkerhetsarbete försvåras. Utredningen har därför föreslagit att de närmare förutsättningarna för tillskapandet av ett heltäckande och sammanhållet regelverk på området samt framtagandet av författningsförslag avseende ett sådant måste utredas i särskild ordning. Mot bakgrund av den tid som en sådan särskild utredning och efterföljande lagstiftningsarbete kan komma att ta och med hänsyn till det stora behov av åtgärder som tidigare har beskrivits, anser utredningen att det redan nu bör vidtas åtgärder genom författningsförslag för att underlätta och effektivisera informationssäkerhetsarbetet.

Med hänsyn till att regeringen har möjlighet att styra statliga myndigheters verksamhet genom förordning lämnas därför i avvaktan på att ett mera sammanhållet och heltäckande regelverk

om informationssäkerhet utretts närmare ett förslag till förordning med grundläggande säkerhetsbestämmelser avseende administrativ och teknisk säkerhet för den statliga verksamheten.

Utredningen har pekat särskilt på att Krisberedskapmyndigheten har utfärdat rekommendationer, förslag till basnivå för IT-säkerhet, benämnt BITS. Dessa rekommendationer innehåller definitioner som rör de delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring detta. Definitionerna följer i huvudsak SIS tekniska rapport Handbok 550: terminologi för informationssäkerhet (2003). De är väl förankrade såväl nationellt som internationellt.

Dessa har, tillsammans med vissa bestämmelser i säkerhetsskyddslagen och säkerhetsskyddsförordningen, utgjort utgångspunkten för bestämmelserna i den förordning som föreslås.

7.7 Övriga författningsförslag

7.7.1 Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633)

Utredningen har valt en bred definition av begreppet informationssäkerhet. Utgångspunkten är EU:s säkerhetsbestämmelser som enligt utredningen utgör ett modernare och mera ändamålsenligt regelverk för informationssäkerheten än det som återfinns i Sverige i dag. Enligt EU:s säkerhetsbestämmelser syftar säkerheten till att främja tillväxt, konkurrens och välfärd. I bestämmelserna talas det om uppgifter som lagras, bearbetas och överförs i elektronisk form och om att säkerheten skall uppfyllas genom krav på konfidentialitet, okränkbarhet och tillgänglighet. Kraven på okränkbarhet och tillgänglighet gäller all informationshantering, oavsett om uppgifterna är hemliga eller inte. Utredningen har tidigare också när den redovisat sin bredare definition av begreppet informationssäkerhet hänvisat till SIS handbok 550: Terminologi för informationssäkerhet. Enligt SIS är begreppet informationssäkerhet mycket brett och omfattar flera underområden som till exempel grundläggande policy, riskhantering samt administrativa och tekniska åtgärder. Enligt såväl SIS som utredningen är informationssäkerhet säkerhet rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spår-

barhet och oavvislighet. Begreppet innefattar såväl IT-säkerhet som säkerhet i administrativa rutiner.

Denna bredare definition som utredningen valt och som utredningen anser att ett nytt regelverk på informationssäkerhetsområdet måste återspeglas i måste ställas mot den legaldefinition av begreppet informationssäkerhet som i dag finns i säkerhetsskyddslagen. Enligt säkerhetsskyddslagen skall säkerhetsskyddet förebygga bland annat att uppgifter som omfattas av sekretess och som rör rikets säkerhet, obehörigen röjs, ändras eller förstörs (informationssäkerhet). Enligt säkerhetsskyddslagen omfattar informationssäkerhet således enbart uppgifter som omfattas av sekretess och som rör rikets säkerhet. Denna legaldefinition av begreppet informationssäkerhet är enligt utredningen därför betydligt smalare än den definition som utredningen förespråkar och som har sin grund i såväl EU:s säkerhetsbestämmelser som i den gängse uppfattningen på informationssäkerhetsområdet.

Mot bakgrund av vad som nu har redovisats anser utredningen att det föreligger skäl att utmönstra den nuvarande legaldefinitionen i säkerhetsskyddslagen av begreppet informationssäkerhet. Begreppet bör ersättas med begreppet sekretessäkerhet som bättre återspeglar vad bestämmelserna i säkerhetsskyddslagen avser. Som en följd av detta bör ändringar i nämnt avseende även göras i säkerhetsskyddsförordningen.

7.7.2 Lagen om elektronisk kommunikation (2003:389)

Utredningen har konstaterat av bestämmelserna i EkomL (2003:389) i nuvarande lydelse i allt väsentligt tar sikte på att skydda den enskildes integritet. Krav på säkerhet är svagt uttryckta och omfattar inte informationssäkerhet i den bredare bemärkelse som utredningen lyfter fram. Detta är en svaghet, särskilt som höga krav på informationssäkerhet snarast främjar integriteten.

Ett viktigt inslag i den statliga politiken har varit att öka tillgängligheten till informationssamhällets växande utbud av tjänster. I takt med att elektronisk kommunikation, framförallt via Internet, används i allt högre utsträckning för såväl transaktioner av affärsmässig karaktär som allt fler samhällsviktiga tjänster för medborgare, företag och myndigheter, så ökar också exponeringen mot och konsekvenserna av haverier i systemen liksom brottsligheten.

För att bibehålla och stimulera fortsatt tillväxt av olika tekniska lösningar och ett varierat tjänsteutbud krävs att användarna har förtroende för att de allmänt tillgängliga kommunikationtjänsterna är säkra och fungerar effektivt samt att användarnas integritet skyddas.

Som utredningen pekar på är den enskilde användaren i allt högre utsträckning beroende av sammankopplade lokala och globala informationssystem och kommunikationsnät. Det är därför viktigt att ansvaret för säkerheten också tydliggörs, det vill säga var gränsen går för det privata åtagandet och när blir det en fråga för staten? Enligt utredningen är det viktigt att lagstiftaren tillhandhåller en reglering som täcker in olika företeelser oberoende av tekniskt medium för kommunikationen. Den som utvecklar och tillhandhåller produkter och tjänster bör rimligen även svara för säkerheten i de levererade systemen eller näten. Slutligen måste den enskilde användaren svara för att utveckla medvetenhet och kompetens så att dennes beteende inte i sig orsakar svåra problem i samband med kommunikation över allmänt tillgängliga nät. Operatörerna av nät och tjänster måste å sin sida ha förmåga att förhindra, upptäcka och reagera på icke acceptabla beteenden, icke avsiktliga avbrott eller störningar i kommunikationen.

Mot denna bakgrund har utredningen övervägt att föreslå förändringar av EkomL i några avseenden. För det första bör EkomL:s tillämpningsområde utvidgas till att omfatta alla former av elektronisk kommunikation, således inte bara den fasta telefonin. Vidare bör möjligheterna att ställa administrativa och tekniska krav på operatörer enligt EkomL utökas och PTS bör ges en starkare roll att utfärda föreskrifter för verkställighet av sådana krav. Slutligen bör möjligheterna till filtrering liksom förutsättningen för hantering av abonnentuppgifter tydliggöras.

I fråga om EkomL:s tillämpningsområde har Riksdagen efter förslag av Trafikutskottet beslutat att utvidga detta (hänvisning). Även om utredningen har synpunkter på vissa formuleringar av dessa ändringar, så finns det i dagsläget inte anledning att aktualisera ytterligare förslag i detta avseende.

När det gäller möjligheterna att tillgodose ökade krav på funktion och teknisk säkerhet m.m. har utredningen haft dialog med PTS. PTS har under utredningsarbetets gång också gjort en framställning till regeringen med förslag till ändringar i EkomL i dessa avseenden. Efter att ha tagit del av dessa förslag väljer utredningen att i princip ställa sig bakom PTS framställan. Utredningen

har således valt att inte lägga några ytterligare förslag så länge som beredning pågår inom Regeringskansliet.

7.8 Standarder för informationssäkerhet

Standarder är privaträttsliga dokument för frivillig användning av parterna på en marknad. Avsikten med standarder är att förenkla och förbilliga tillverkning och handel. Standardiseringsarbete kan bedrivas i flera olika former. Den erkända standardiseringen bedrivs internationellt inom ISO, International Organization for Standardization, IEC, International Electrotechnical Commission samt inom ITU, Internationella Teleunionen. I dessa organisationer är de nationella standardiseringsorganen medlemmar. Svenska medlemmar i dessa organisationer är SIS, Swedish Standards Institute, SEK, Svenska Elektriska Kommissionen respektive ITS, Informationstekniska standardiseringen.

I olika sammanhang använder sig lagstiftaren av standarder. Man gör till exempel standarderna lagligen bindande eller man anger att en viss standard är exempel på en tillfredsställande lösning. Ofta hänvisas till standarder vid offentlig upphandling.

Standardiseringen på informationssäkerhetsområdet har i dag kommit mycket långt. De internationella standardiseringsorganen har till sitt förfogande experter inom varje relevant delområde inom informationssäkerhet, inklusive kryptologiområdet.

Bland standarder och utvecklingsprojekt för standarder inom SC 27 (ISO/IEC) kan nämnas:

- SIS LIS-projekt (Ledningssystem för informationssäkerhet),
- *Common Criteria* för evaluering och certifiering,
- Standarder för kryptologiska algoritmer och protokoll.

Standardiseringsgrupperna arbetar i en öppen process i den meningen att alla kan bli medlemmar. Flera standardiseringsorganisationer publicerar sina standarder fritt, andra måste man betala för. Deras arbete utsätts för en omfattande granskning av kryptologer från vetenskap, industri och myndigheter. Att konstruera kryptografiska lösningar är mycket svårt. Det krävs dessutom lång tid och en oberoende granskning från flera parter för att en publik kryptoalgoritm eller ett säkerhetsprotokoll skall få nödvändig tillit.

Säkerhetsrelaterade faktorer som är viktiga för ett företag som utvecklar en säkerhetslösning är bland andra:

- Val av plattform (hur skyddas den? IDS, Brandväggar, VPN, antivirus),
- Val av standarder inklusive optioner (kryptoalgoritmer, hash-funktioner, signaturscheman, nyckellängder och så vidare)
- Införandet av säker kod,
- Kvalitetssäkring,
- Användarvänlighet; en användare skall inte behöva göra aktiva val för att få hög säkerhet.

Nämnden för elektronisk förvaltning har till uppgift att stödja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte mellan myndigheter samt mellan myndigheter och enskilda genom att bland annat besluta om standarder eller liknande krav som skall vara gemensamma för det elektroniska informationsutbytet för myndigheter. Nämnden skall bistå med information och utarbeta riktlinjer, samt verka för att det på marknaden för informationsteknik tillhandahålls tjänster och produkter till stöd för elektroniskt informationsutbyte.

Enligt vad utredningen erfarit planerar Nämnden för elektronisk förvaltning att utge särskilda föreskrifter för informationssäkerhet.

7.8.1 Metodik för kvalitets- och kompetensutveckling

Informationssäkerhet är ytterst en fråga om kvalitetstänkande. När det gäller system för hantering och utbyte av elektronisk information så är det grundläggande att dessa bygger på standarder. En praktisk förutsättning är interoperabilitet. En kostnadsmässig fördel är att standarder främjar konkurrens på lika villkor bland leverantörer. Kunden blir inte låst till en leverantör. Det går att blanda produkter från flera leverantörer. Produkterna kan effektivt uppgraderas då standarder vidareutvecklas för att möta nya hot eller dra nytta av de senaste landvinningarna inom forskningen.

Det är förklarligt att det finns brister i informationssäkerheten hos många organisationer. Även om ledningen skulle vara medveten om behovet av hög informationssäkerhet är det inte säkert att man vet hur man skall uppnå detta. Med en kvalitetsstandard att arbeta efter finns det betydligt bättre förutsättningar att nå målet. Det finns flera standarder inom informationssäkerhetsområdet.

EU har från 2002 pekat ut *Common Criteria*, ISO/IEC 15408, och Ledningssysten för informationssäkerhet, ISO/IEC 17799 och SS 62 77 99-2, som grunder för informationssäkerhet. Utredningens uppfattning är att staten bör gå i bräschen för en bred användning av standarder inom i princip all statlig verksamhet.

7.8.2 Common Criteria

Common Criteria, ISO/IEC 15408, är en internationell standard för att ställa krav på och utvärdera säkerheten hos IT-produkter och IT-system i dess användningsmiljö. *Common Criteria* är ett ramverk för hur man beskriver de funktionella kraven på IT-säkerhet i en produkt, inte en kravställning i sig. Syftet är att först utveckla en kravbild, för att sedan kunna utvärdera produkten i förhållande till ställda krav. Metoden för att genomföra utvärderingen är standardiserad och kan ske med varierande noggrannhet (assuransnivåer) och kan därmed genomföras med varierande kostnad och resultera i olika grad av tillit till produkten. Syftet är att kunna utvärdera i förhållande till ställda krav.

Kraven ställs utifrån risker och hot för produkten och dess användning. En köpare skall kunna lita på att certifierade produkter och program fyller högt ställda och allmänt accepterade krav.

En utvecklare eller leverantör beskriver hur detta skall uppnås genom att fastställa nödvändiga säkerhetsmål. En tredje part, en utvärderingsorganisation, testar och utför säkerhetsvärderingen. Validering utförs av ett certifieringsorgan och om uppställda krav är uppfyllda kan produkten certifieras. *Common Criteria* har sju assuransnivåer.

I huvudsak används *Common Criteria* för att säkerhetsklassa en produkt (IT-system) i sin miljö med avseende på berörda lagar, risk och sårbarheter rörande produkten, implementeringsplan och utvärdering av förverkligandet utifrån ställda krav. Varje komponent i produkten granskas och dess beroende kartläggs och klassas. I granskningen görs bedömning och tester av funktioner, design och konsekvens.

Common Criteria Recognition Arrangement (CCRA) är en samverkan mellan nationer där det övergripande målet är att höja den nationella säkerheten genom att använda Common Criteria som ett verktyg för kravställning och granskning och verka för att antalet säkra IT-produkter ökar.

Sverige är medlemsnation i *Common Criteria Recognition Arrangement*, som är ett avtal för ömsesidigt erkännande av certifikat utgivna av medlemsnationerna. Avtalet innebär att då certifiering anges som ett krav på en IT-säkerhetsprodukt vid offentlig upphandling i ett nation, måste denna nation acceptera certifikat utställda av de övriga nationerna, utan ytterligare krav på granskning av den upphandlande nationen. Det ömsesidiga erkännandet inom CCRA omfattar dock enbart de lägre assuransnivåerna (1–4). Begränsningar medges även för produkter som ska hantera t ex information som är av nationellt säkerhetsintresse.

Regeringen konstaterade i propositionen Fortsatt förnyelse av totalförsvaret (prop. 2001/02:10) att samhället i stort och totalförsvaret i synnerhet behöver ha en god uppfattning om vilken säkerhetsnivå olika IT-produkter medger. Därför ansåg regeringen att det behövs ett system för utvärdering och certifiering av produkter. Under hösten 2002 blev Styrelsen för ackreditering och teknisk kontroll, Swedac, svensk signatär.

Försvarets materielverk, FMV, har fått regeringens uppdrag att bygga upp en svensk certifieringsordning för CCRA.

Mot bakgrund av erfarenheter från andra länder inom CCRA, är det troligt att Försvarsmakten och andra myndigheter med mycket höga sekretesskrav, kommer att vara de viktigaste intressenterna för certifierade produkter. Tillgång till certifierade produkter underlättar samtidigt för alla myndigheter, företag och andra som önskar upphandla produkter med hög säkerhet.

7.8.3 Ledningssystem för informationssäkerhet, LIS

Ledningssystem för Informationssäkerhet (LIS) är en anvisning för hur man åstadkommer ett ledningssystem, inte ledningssystemet i sig. Den omfattar hela informationssäkerhetsbegreppet, och fokuserar på de risker och hot som kan uppkomma inom en organisation.

LIS bygger på den ursprungliga brittiska standarden BS 7799, och består av två delar. Den första delen, riktlinjerna, är både svensk och internationell ISO-standard, SS-ISO/IEC 17799. Denna del kan sägas vara bör-krav för hur man skapar en säker informationshantering. Den innehåller råd om säkerhetspolicy, organisatorisk säkerhet, klassificering och styrning av tillgångar, personal och säkerhet, fysisk och miljörelaterad säkerhet, styrning

av kommunikation och drift, styrning av åtkomst, systemutveckling och systemunderhåll, kontinuitetsplanering samt efterlevnad.

Den andra delen, specifikationen, finns som svensk standard SS 62 77 99-2, vilken också företag kan låta sig certifieras mot. Andra länder, förutom Storbritannien, som infört denna som nationell standard är Norge, Irland, Australien, Nya Zeeland och Nederländerna. Den tillämpas också i bland annat Finland, Tyskland, USA, Japan, Brasilien, Kina, Taiwan och Sydafrika. Denna del kan sägas utgöra skall-kraven på ett ledningssystem för informationssäkerhet.

LIS beskriver ledningssystemet med följande innehåll:

- Dokumenterad informationssäkerhetspolicy på en övergripande nivå, med verksamhetskraven som utgångspunkt. Den beskriver även ledningens viljeinriktning.
- Utpekande av ansvariga (roller). Den visar på vilka säkerhetsprocesser som skall/bör göras och målen för dessa.
- Struktur för anvisningar och regler för säkerhetsåtgärder som är anpassade efter verksamhetens behovsbild.
- Definition av en modell för riskanalys och riskhantering.
- Definition av en modell för uppföljning och ständiga förbättringar av säkerhetsarbetet.
- Rutiner för kontinuerliga revisioner av redan införda säkerhets- och riskhanteringsrutiner.
- Ett strukturerat sätt att sprida kunskapshöjande insatser till medarbetarna i den egna verksamheten.

Viktiga utgångspunkter är att LIS utgår ifrån den egna verksahetens behov av skydd. Kärnan i LIS baseras på regelbundet återkommande riskanalyser. Hänsyn tas till intressenters behov. Verksamhetens ledning ges ett tydligt ansvar för informationssäkerheten. En förutsättning för LIS är att det inte ses som ett utanförskap i förhållande till övriga verksamhetsprocesser. Den ger grunden för tillämpning av angelägna säkerhetskrav och rutiner

LIS används med framgång inom flera större svenska företag. Detta tillsammans med erfarenheten att framstående nationer använder standarden nationellt, motiverar enligt utredningen att staten bör använda LIS inom den statliga verksamheten.

7.8.4 Statskontorets OffLIS

OffLIS är Statskontorets ”mallregelverk”, ett startpaket för att utforma LIS vid 24-timmarsmyndigheter. OffLIS innehåller en rekommenderad mall för en organisations ledningssystem för informationssäkerhet, baserat på LIS.

OffLIS ingår i ett databasverktyg i MS Access, som stöd för hela säkerhetsprocessen från upprättande av en organisations regelverk till stöd för uppföljning av säkerheten. Den primära målgruppen är alla som arbetar aktivt med informationssäkerhet i en organisation, det vill säga primärt informationssäkerhetschefer, IT-säkerhetschefer, IT-säkerhetssamordnare eller motsvarande. Även om OffLIS är utformat med 24-timmarsmyndigheter som målgrupp, kan det oftast utan större besvär även anpassas till andra organisationers verksamhet.

OffLIS innehåller:

- Anvisningar för utformning av policy för informationssäkerhet.
- Mall till riktlinjer för informationssäkerhet. OffLIS-mallen kan enkelt anpassas för att utforma ett eget regelverk med önskad grundskyddsnivå för organisationen.
- Klassificeringsmodell för att definiera önskad grundskyddsnivå genom styrning av skyddsåtgärder beroende på nivå av sekretess, riktighet och tillgänglighet.
- Åtgärdskrav för valt informationsobjekt, system eller dylikt enligt genomförd klassificering.
- Stöd för informationsspridning av policy och övriga regler genom många möjligheter att skikta regelverket, till exempel:
  - indelning på riktlinjer och anvisningar,
  - rollstyrning av databasens innehåll av regler,
  - utformning av ”ledningssammanfattning” och annat
  - presentationsmaterial från regelverket.

Utredningen anser att OffLIS bör utgöra ett rekommenderat stöd från staten vid införande av LIS i myndigheters verksamhet.

7.8.5 BITS

BITS är Krisberedskapsmyndighetens, KBM, nuvarande rekommenderade basnivå för IT-säkerhet. Den anger en rekommenderad lägsta säkerhetsnivå för IT-system som bedöms nödvändig för att

upprätthålla en organisations normala verksamhet även under fredstida kriser.

BITS är en rekommendation ifråga om den basförmåga för informationssäkerhet som skall finnas hos myndigheter, men som definieras av varje enskild myndighet efter risk- och sårbarhetsanalys för den egna verksamheten.

Krisberedskapsmyndighetens rekommendationer har som utgångspunkt haft olika standarder och standardiseringssträvanden som förekommit på olika håll, men anpassats och begränsats för att ge ett konkret stöd i arbetet med att uppnå basnivån. Ambitionen är att få BITS att konvergera mot LIS eller OffLIS där parallellitet finns. Grundtanken att definiera en lägsta nivå för IT-säkerhet kvarstår.

Medan standarden LIS är en metod – den anger vad som behöver beaktas, är BITS och OffLIS verktyg – de anger hur säkerheten skall åtgärdas. BITS är inriktat mot IT-säkerhet och behöver breddas till att omfatta hela begreppet informationssäkerhet, samt kompletteras med krav på process för styrning och underhåll av informationssäkerhetsarbetet. OffLIS tar ett större grepp och omfattar rekommenderade åtgärder för en organisations hela informationssäkerhetsområde i enlighet med LIS.

OffLIS hänvisar naturligt till BITS som ett stöd för införande av konkreta systeminriktade åtgärder gällande lagstiftning och förekommande rekommendationer. Arbete pågår nu för att få en fullständig integration av BITS och Statskontorets OffLIS.

Ett resultat som blir mera heltäckande och inte enbart fokuserar på IT-säkerhet skulle kunna bli en föreskrift för alla myndigheter. Att få fram en bra basnivå för informationssäkerhet på alla myndigheter skulle också kunna underlätta Säkerhetspolisens författningsreglerade arbete med rådgivning och kontroll.

7.8.6 Datainspektionen – säkerhet för personuppgifter

Datainspektionens allmänna råd preciserar personuppgiftslagens (1998:204) krav på säkerhet vid behandling av personuppgifter. Enligt 31 § ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter. Den som behandlar personuppgifter bör tänka på att kartlägga hotbilden, sätta mätbara mål för säkerhet och skapa en fungerande organisation för säkerhet. Det innebär bland annat att skaffa

adekvat utrustning, upprätta regler och rutiner, informera och utbilda kontinuerligt samt att följa upp att regler och rutiner efterlevs och respekteras. Säkerheten skall testas regelbundet.

Ansvaret för säkerheten vid behandling av personuppgifter är enligt personuppgiftslagen en personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen och medlen för personuppgifter. Den faktiska behandlingen av personuppgifter kan överlåtas till annan som då blir att betrakta som personuppgiftsbiträde. Denne får behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet och den ansvarige skall upprättas. I avtalet skall säkerhetåtgärderna vid behandlig av personuppgifter regleras.

Det är angeläget att Datainspektionens allmänna råd relateras och närmas till den internationella standarden SS-ISO/IEC 17799. Enligt vad utredningen erfarit kommer Datainspektionen att genomföra en översyn av de allmänna råden i bland annat detta syfte under 2005.

7.8.7 Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd

I Rikspolisstyrelsens föreskrifter och allmänna råd ges tillämpningsföreskrifter till säkerhetsskyddslagen när det gäller informationssäkerhet, tillträdesskydd och säkerhetsprövning. Föreskrifterna gäller för statliga myndigheter samt för kommuner och landsting. Bestämmelserna om informationssäkerhet gäller för uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet (hemliga uppgifter).

I den omarbetade föreskrift, som trädde i kraft den 1 februari 2005 (RPSFS 2004:11, FAP 244-1) har bestämmelserna om informationssäkerhet delats upp i två delar. Ett kapitel behandlar informationssäkerhet för hemliga handlingar i skrift eller bild och ett kapitel informationssäkerhet för hemliga uppgifter i IT-system.

Av föreskrifterna framgår bland annat att myndighetens chef skall fastställa mål och riktlinjer för IT-säkerheten, liksom instruktioner för användning, förvaltning och drift av IT-system som används för hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. För ett sådant IT-system skall finnas en av

myndighetens chef utsedd person som ansvarar för säkerheten i systemet.

Föreskrifterna innehåller krav att sådana IT-system skall vara försedda med tekniska eller administrativa åtgärder för identifiering av användaren, verifiering av identiteten, styrning av åtkomsträttigheter samt registrering av aktiviteter (behörighetskontroll) och loggning av bland annat användaridentitet och aktiviteter av betydelse för säkerheten i systemet (säkerhetsloggning). Bestämmelserna innehåller vidare bestämmelser om bland annat skydd mot skadlig kod, intrångsskydd, incidenthantering och säkerhetskopiering.

Föreskrifterna är framtagna i samarbete med andra berörda myndigheter, bland annat Försvarsmakten, Statskontoret och Krisberedskapsmyndigheten. Föreskrifterna skiljer sig delvis från de föreskrifter som Försvarsmakten meddelat, men man har strävat efter att resultatet skall bli likartat. En annan ambition har varit att föreskrifterna inte skall stå i strid med de rekommendationer som lämnas i BITS för att underlätta för de myndigheter som valt att följa dessa. Rikspolisstyrelsen ställer dock, av naturliga skäl, högre krav i flera avseenden.

7.8.8 Övriga standarder

En standard, som inte används i Europa i särskilt stor utsträckning, är ISO/IEC 13335. Den har utvecklats från den äldre ISO/IEC TR 13335 – *Guidelines for the Management of IT Security* (GMITS), till den nyare ISO/IEC 13335 – *Management of Information and Communications Technology Security* (MICTS).

GMITS har haft som syfte att ge vägledning och instruktioner för styrning och kontroll av informationssäkerhet inom en organisation. Den utgjorde främst ett planeringsverktyg för IT-säkerhetsarbetet, innehöll och presenterade grundläggande koncept och modeller vilka är väsentliga för en introduktion till styrning och kontroll av IT-säkerhet. Koncepten och modellerna utvecklades ytterligare i kompletterande delar.

GMITS användes främst av informationssäkerhetschefer för att uppnå och bibehålla uppsatta säkerhetsnivåer inom sekretess, integritet, tillgänglighet, spårbarhet och tillförlitlighet för informationssäkerhetsarbetet. Den var också relevant för IT-chefer med

ansvar speciellt inom områdena inköp, design, implementering och underhåll av IT-tjänster. GMITS bestod av fem delar.

MICTS är den nyare standarden, som är under utarbetande och ännu ej slutgiltigt fastställd. När den är klar kommer den att bestå av två delar. Del 1 av MICTS ger en översikt över koncept och modeller som används vid ledning av säkerhet inom informations- och kommunikationsteknik. Denna kommer att ersätta GMITS del 1 och 2.

Del 2 av MICTS beskriver tekniker för riskhantering av säkerhet inom informations- och kommunikationsteknik lämpliga för användning vid ledning. Denna kommer att ersätta GMITS del 3 och 4.

Dokumenten MICTS syftar till att, i viss utsträckning på övergripande nivå, informera om ledning och styrning av informationssäkerhet, hur man genomför riskanalyser och väljer skyddssystem. De syftar också till att utveckla och genomföra en övergripande strategisk plan och policy för exempelvis en nation beträffande dess ledning inom informations- och kommunikationsteknik. Den är också till hjälp om man önskar samordna eller planera flera länders olika strategier till en gemensam plan.

Användningsområdet är i första hand för informations- och kommunikationsområdet inom industrin. Dokumenten exemplifierar hur man tar fram strategi för olika databaser. MICTS ska även kunna användas för att samordna flera områden/kommuner/nationer som redan har strategier och olika policy, till en gemensam strategisk plan och policy.

En trolig utveckling av ISO IEC 13335 är att dessa standarder kommer att föras över till samma standardfamilj som LIS i nummerserien 27000.

7.9 Målstruktur för informationssäkerhet

Till informationssäkerhet hör att förebygga störningar eller funktionsbortfall, att förbereda sig för att kunna hantera störningar när de uppträder, samt att kunna agera operativt vid störningar. Till säkerhetsperspektivet hör även att utvärdera och återföra erfarenheter för en ökad robusthet och förbättrad säkerhet i framtida verksamhet.

Finansdepartementet har formulerat gemensamma principer för mål, med generella kriterier vid formuleringen av mål. De principer som formuleras i en målstruktur bör avse mål som omfattas av

budgetprocessen men också ha bäring på mål som formuleras i andra sammanhang. Målstrukturen kan ses som en produktionskedja. Av målet skall framgå vad som skall uppnås. Målen kan avse såväl effekter som prestationer.

Den verksamhetsstruktur som gäller för svensk statlig förvaltning innebär i regel att mål formuleras på flera nivåer. Strukturen syftar till att tydliggöra hur verksamheter på skilda nivåer bidrar till att uppfylla målen för ett politikområde. Som en följd av detta kommer målen att skilja sig i precision mellan nivåerna.

För att målen skall kunna tjäna som ett styrinstrument är det nödvändigt att de är realistiska och möjliga att nå av de som ansvarar för genomförandet. Målen måste också uppfattas som relevanta för att accepteras och godkännas av såväl riksdag som myndigheter.

Informationssäkerhet kan definieras som ett verksamhetsområde eller en del av ett politikområde. Det berör i så fall många politikområden och flera utgiftsområden. Här kan man se informationssäkerhet som en förutsättning för övriga verksamheter. Det ställer särskilda krav på strategier för hur en systematisk och sektorsövergripande uppföljning skall gå till.

Ansvarsprincipen är en naturlig utgångspunkt i arbetet med informationssäkerhet, det vill säga den som har ansvar under normalt fungerande verksamhet har det i full utsträckning även vid incidenter och andra störningar. Av ansvarsprincipen följer även att den som är ansvarig för verksamheten även ansvarar för planeringen av förebyggande och förberedande insatser. Ansvaret för informationssäkerhet i den offentliga verksamheten kan inte läggas på något fristående tillsyns- eller underhållsorgan. Däremot bör det självfallet vara möjligt att upphandla tjänster för att utföra nödvändiga åtgärder för en god informationssäkerhet.

Mål för informationssäkerhet bör enligt utredningen formuleras för den statliga verksamheten som en del i den finansiella styrningen av statsförvaltningen. Mål för informationssäkerhet bör även formuleras för samhällsviktig verksamhet som inte drivs i statlig regi.

Tre typer av mål bör formuleras för informationssäkerhet:

- Överordnade mål som avser krav på prestationsförmåga eller säkerhet för samhällskritisk verksamhet
- Mål som avser krav på tillämpning av standarder, viss lägsta prestationsförmåga – dels normalt, dels under störda förhållanden

- Mål som avser kompletterande åtgärder för informationssäkerhet

Informationssäkerhet har tvärsektoriell karaktär. Ett helhetsperspektiv kan vara svårt att applicera i den sektorsuppdelade struktur som kännetecknar den statliga verksamheten. Helhetssynen kan också försvåras av att steget mellan överordnade mål och regleringsbrevsmål är långt. Möjligheten för enskilda myndigheter att få en konkret bild av sin respektive deluppgift i relation till övergripande gemensamma mål är därför begränsad.

Det är angeläget att samordna målformuleringarna inom näraliggande verksamheter. Man måste ta hänsyn till de beroendeförhållanden som finns mellan olika delar av ett samhällsviktigt område, då man utformar de samlade målen för ett sådant område. En viss nivå för informationssäkerhet inom den tekniska infrastrukturen förutsätter att målen vad gäller säkerhet i elförsörjningen och telekommunikationerna balanserar mot varandra.

I målstrukturen för informationssäkerhet behöver övergripande och gemensamma effektmål kunna brytas ner i flera steg och konkretiseras innan myndighetsspecifika prestationsmål formuleras. Operativa prestationsmål måste kunna härledas ur överordnade mål och kunna följas upp. En logisk spårbar målstruktur är en förutsättning för att kunna revidera verksamheten.

Högst upp i målhierarkin, på politikområdesnivå, bör finnas övergripande mål för informationssäkerhet. På denna nivå bör målformuleringen omfatta de underliggande verksamhetsområdena. Målformuleringen blir här generell till sin karaktär.

Under dessa övergripande mål, på verksamhetsområdesnivå, bör däremot finnas mål för olika samhällsviktiga verksamheter. På nästa nivå, det vill säga verksamhetsgren, bör det finnas operativa mål som kan vara ganska kortsiktiga – ett till tre år. Operativa mål kallas också prestationsmål.

På nivån under de operativa målen återfinns mål på myndighetsnivå.

Resonemanget kan sammanfattas på följande sätt:

- Politikområde (effektmål)
- Verksamhetsområde (effekt- eller prestationsmål)
- Verksamhetsgren (prestationsmål)
- Myndighetsnivå (prestationsmål)

Utgiftsområde 6 Försvar samt beredskap mot sårbarhet består i dag av två politikområden, Totalförsvar samt Skydd och beredskap mot olyckor och svåra påfrestningar. Informationssäkerhet skulle kunna ingå som en del av politikområdet Skydd och beredskap mot olyckor och svåra påfrestningar, eller ingå som en del i flera politikområden. Teoretiskt skulle det även kunna utgöra ett eget politikområde.

Utredningen förordar i första hand att informationssäkerhet ses som ett verksamhetsområde, ingående i flera politikområden.

Det finns olika sätt att konkretisera en ny målstruktur. Valet av hierarki blir beroende av vad som skall framhållas, vilka effekter som eftersträvas och hur effektsamband skall tydliggöras. Målstrukturen behöver anpassas till respektive organisation.

Politikområde

Här bör övergripande principer redovisas som skall vara styrande för en helhetssyn på informationssäkerhet.

Verksamhetsområden

Informationssäkerhet bör enligt utredningen vara ett verksamhetsområde. Ett exempel på ett målresonemang skulle kunna vara kravet på robusthet och säkerhet inom samhällsviktiga verksamheter och övergripande mål som avser krav på prestationsförmåga eller tillgänglighet. Övergripande krav bör formuleras i måltermer, inte som krav på att vissa tekniska lösningar skall användas.

Verksamhetsgrenar

Verksamhetsområdet skulle kunna delas in i ett antal verksamhetsgrenar. En sådan indelning kan spegla dels de viktigaste beståndsdelarna i informationssäkerhet, dels att informationssäkerhet hör hemma inom ett flertal verksamhetsområden.

Säkerhetsmål kan vara generella krav på tillämpning av standarder eller krav på en lägsta godtagbara funktionsförmåga, dels normalt, dels under störda förhållanden. Vid koncessioner bör säkerhetskrav arbetas in i koncessionsvillkoren.

Myndighetsnivå

Under nivån verksamhetsgren formuleras mål på myndighetsnivå för informationssäkerhet. Målen kan formuleras som operativa prestationsmål, krav på tillgänglighet, specifik tillämpning av standarder, krav på säkerhetspolicy, samt krav på tester och revision av säkerheten.

Finansiell styrning

Det finns flera sätt att finansiera en offentligt bedriven verksamhet eller en offentligt reglerad verksamhet som bedrivs av en annan huvudman än staten. Det kan ske genom skattefinansiering i kombination med anslag eller bidrag till verksamheten. Ett annat alternativ, främst för reglerad verksamhet som bedrivs av annan än staten, genom offentligrättsligt reglerade avgifter som endast får användas för att finansiera en viss verksamhet eller ett visst åläggande. Ett tredje alternativ är att finansiera verksamheten genom försäljning av varor och tjänster på en marknad. Ytterligare ett fjärde alternativ kan vara att anslå medel i ett särskilt samlat anslag för att finansiera riktade insatser för särskilda ändamål inom olika utgifts- eller politikområden.

Utredningen förordar att informationssäkerhet för statens del ses som ett verksamhetsområde. Redan detta innebär ett visst ställningstagande. Med utgångspunkt i ansvarsprincipen är det rimligt att finansiering av informationssäkerhet i huvudsak sker genom ordinarie anslag för verksamhetsområdet till respektive myndighet. Det bör enligt utredningen vara huvudprincipen för finansieringen och den finansiella styrningen av informationssäkerhet.

Att ta ut avgifter som endast får användas för att finansiera informationssäkerhet kan vara möjligt inom till exempel teknisk infrastruktur. Post- och telestyrelsen (PTS) har en lång och positiv erfarenhet av denna form av finansiell styrning inom teleområdet.

Att sälja tjänster för offentlig informationssäkerhet och därigenom finansiera verksamhet kan endast i starkt begränsad omfattning vara ett alternativ. Om informationssäkerhet kan säljas som en tjänst hör den normalt hemma på en marknad, där motiv ofta saknas för mera omfattande offentliga verksamhet.

Möjligheten att anslå medel i ett särskilt samlat anslag för att finansiera riktade insatser för särskilda ändamål inom olika utgifts-

och politikområden finns i praktiken redan genom den ekonomiska planeringsramen, den s.k. civila ramen. Den har tidigare motiverats för att kunna finansiera insatser i civilt försvar som en förberedelse inför höjd beredskap. Under senare år har den i ökad utsträckning fått medverka till finansieringen av åtgärder för en bättre krisberedskap, också inom området informationssäkerhet. Den finansierar således delar av verksamheten hos Sitic – PTS:s incidenthanteringsfunktion, Försvarets radioanstalts teknikkompetensfunktion, samt uppbyggnaden av en certifieringsfunktion enligt Common Criteria vid Försvarets materielverk, särskilda forskningsmedel vid Krisberedskapsmyndighen samt kommunernas planeringssystem inför extraordinära händelser.

Det är enligt utredningen motiverat att även i framtiden – särskilt för ändamål som kan ses som långsiktiga investeringar i en högre informationssäkerhet – behålla möjligheterna till kompletterande finansiering av informationssäkerhet via den så kallade civila ramen. Utredningen avser att återkomma till dessa frågor i sitt organisatoriska betänkande.

7.10 Utredningens slutsatser angående styrmedel

Enligt utredningen är informationssäkerheten en angelägenhet för hela samhället. Behovet av en tillfredställande informationssäkerhet är till exempel inte begränsat till verksamheter som är av betydelse för rikets säkerhet eller skyddet mot terrorism. Behovet är inte heller begränsat till information som är hemlig enligt sekretesslagen eller som är känslig ur ett integritetsperspektiv och så vidare. Behovet av säkerhet för information kan, som utredningen tidigare har pekat på, göra sig lika starkt gällande även på andra områden. Utredningen har därför förordat en bred definition av begreppet informationssäkerhet med utgångspunkt i EU:s säkerhetsbestämmelser. Enligt dessa syftar informationssäkerheten till att främja tillväxt, konkurrens och välfärd. För uppgifter som lagras, bearbetas och överförs i elektronisk form skall säkerheten uppfyllas genom krav på konfidentialitet, okränkbarhet och tillgänglighet.

I detta kapitel har utredningen redogjort för ett flertal författningar av särskilt intresse på informationssäkerhetsområdet. Av redogörelsen framgår att bestämmelser om informationssäkerhet finns i en mängd olika författningar. Ett heltäckande och sammanhållet regelverk på informationssäkerhetsområdet som motsvarar

utredningens bredare definition av begreppet informationssäkerhet saknas dock. Enligt utredningen föreligger det därför ett behov av ett utvidgat, mera samanhållet och heltäckande regelverk på informationsområdet.

Utredningen har pekat på vad som skulle kunna vara möjliga vägar att gå för att åstadkomma ett sådant regelverk. En väg skulle kunna vara att utöka tillämpningsområdet för nuvarande säkerhetsskyddslagstiftning. En annan väg skulle kunna vara en helt ny lag på informationssäkerhetsområdet. Framtagandet av ett sådant regelverk som utredningen anser att det finns ett stort behov av måste dock föregås av en mycket mer omfattande och djupare analys än vad denna utredning har möjlighet att göra. Frågan om ett mera sammanhållet och heltäckande regelverk på informationssäkerhetsområdet måste därför utredas i särskild ordning.

Utredningen anser dock att den har stöd för att redan nu föreslå lagstiftningsåtgärder för att råda bot på vissa brister hos dagens regelverk. Dels föreslår utredningen en ny förordning om vissa åtgärder för informationssäkerhet hos staten. Dels föreslår utredningen att begreppet informationssäkerhet utmönstras ur säkerhetsskyddslagstiftningen för att ersättas med begreppet sekretessäkerhet.

Enligt utredningen finns starka motiv för att stärka säkerheten i nätsäkerhetsrelaterade frågor. Riksdagens Trafikutskott har också tagit vissa initiativ i dessa frågor och från 1 juli, 2005 gäller utvidgade tillämpningsbestämmelser för säkerheten. Enligt utredningen mening handlar det därutöver om att förstärka möjligheterna att ställa tydligare krav på leveranssäkerhet och kvalitet. Andra aspekter av säkerheten handlar om filtreringsfrågor samt hantering av vissa abonnentuppgifter. Utredningen stödjer Post- och telestyrelsens ambitioner i denna fråga.

Standardiseringen på informationssäkerhetsområdet har i dag kommit långt. Informationssäkerhet är ytterst en fråga om kvalitetstänkande. När det gäller hantering och utbyte av elektronisk information är det grundläggande att dessa bygger på standarder. Fördelarna är många. Utredningens uppfattning är att staten bör gå i bräschen för en bred användning av standarder inom i princip all statlig verksamhet.

Försvarets materielverk har sedan tidigare ett uppdrag att bygga upp en svensk certifieringsordning för *Common Criteria*. Mot bakgrund av erfarenheter från andra länder är det troligt att Försvarsmakten och andra myndigheter med mycket höga sekretesskrav,

kommer att vara de viktigaste intressenterna för certifierade produkter och program. Tillgång till certifierade produkter underlättar samtidigt för alla myndigheter, företag och andra som önskar upphandla produkter med hög säkerhet.

Ledningssystem för Informationssäkerhet (LIS) är en anvisning för hur man åstadkommer ett ledningssystem, inte ledningssystemet i sig. Den omfattar hela informationssäkerhetsbegreppet och fokuserar på de risker och hot som kan uppkomma inom en organisation. Tillämpning leder till förbättrade administrativa och tekniska rutiner. LIS används med framgång inom flera större svenska företag. Detta tillsammans med erfarenheten att framstående länder använder standarden nationellt, motiverar enligt utredningen att myndigheterna bör tillämpa LIS för att uppnå en god nivå på informationssäkerheten i statens verksamhet.

OffLIS är Statskontorets ”mallregelverk”, ett startpaket för att utforma LIS vid 24-timmarsmyndigheter. Utredningen anser att OffLIS bör utgöra ett rekommenderat stöd från staten vid införande av LIS i myndigheters verksamhet. Det är också angeläget att datainspektionens allmänna råd relateras och närmas till LIS. Enligt vad utredningen erfarit kommer Datainspektionen att genomföra en översyn av de allmänna råden i bland annat detta syfte under 2005.

BITS är Krisberedskapsmyndighetens, KBM, nuvarande rekommenderade basnivå för IT-säkerhet. Medan LIS är en metod – den anger vad som behöver beaktas, är BITS och OFFLIS verktyg – de anger hur säkerheten skall åtgärdas. BITS är inriktat mot IT-säkerhet och måste breddas till att omfatta hela begreppet informationssäkerhet, samt kompletteras med krav på process för styrning och underhåll av informationssäkerhetsarbetet.

Utredningen konstaterar att ett arbete numera pågår för att påskynda en fullständig integration av BITS och Statskontorets OffLIS. Viktigt är att resultatet blir mera heltäckande och inte enbart fokuserar på IT-säkerhet. Det skulle därmed kunna utgöra underlag för en föreskrift för alla myndigheter.

Målstruktur för informationssäkerhet

Till informationssäkerhet hör att förebygga störningar eller funktionsbortfall, att förbereda sig för att kunna hantera störningar, samt att kunna agera operativt vid störningar. Till säkerhets-

begreppet hör också att utvärdera och återföra erfarenheter för en ökad robusthet och förbättrad säkerhet i framtida verksamhet.

Den verksamhetsstruktur som finns inom svensk statsförvaltning innebär i regel att mål formuleras på flera nivåer. Strukturen syftar till att tydliggöra hur verksamheter på skilda nivåer bidrar till att uppfylla målen i ett politikområde. Som en följd av detta skiljer målen sig i precision mellan nivåerna.

Informationssäkerhet kan formuleras som ett verksamhetsområde eller en del av ett politikområde. Det berör i så fall många politikområden och flera utgiftsområden. Här kan man se informationssäkerhet som en förutsättning för övriga verksamheter. Utredningen förordar i första hand att informationssäkerhet ses som ett verksamhetsområde.

8 Kompetensfrågor

8.1 Säkerhetsmedvetande

Informationstekniken reformerar världen. På kort tid har tillgång till datorer och förmåga till kommunikation mellan datorer blivit tillgängliga för de allra flesta. För tio år sedan låg datoranvändningen i hemmen på en låg nivå. De allra flesta saknade tillgång till Internet. Den enda egentliga risken var att datavirus kunde spridas via smittade disketter – datavirus som var harmlösa med dagens mått mätt.

I dag är läget annorlunda. De flesta hushåll är uppkopplade mot Internet varje dag, varav många dygnet runt med bredbandsuppkoppling. Riskerna har också förändrats. Datavirus som sprids med disketter förekommer nästan inte alls. Nu är det datamaskar som på bara några timmar sprider sig jorden runt och kan orsaka skador för miljardbelopp. Trojaner är i dag ett reellt hot, där angripare kan skaffa sig kontroll över till synes skyddade datorer. Förutom den skada detta kan förorsaka datorns innehavare, kan förövaren utnyttja den angripna datorn för fortsatta attacker mot andra över Internet.

Utredningen utgår ifrån SIS definitioner av begreppet informationssäkerhet. Det innebär att informationssäkerhet definieras som säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spårbarhet och oavvislighet. Begreppet innefattar såväl teknisk IT-säkerhet som säkerhet i administrativa rutiner.

Under åren efter millennieskiftet har det allmänna säkerhetsmedvetandet vid IT-användning höjts.

Post- och telestyrelsen, PTS, har sedan 2002 ett uppdrag att sammanställa information om Internetsäkerhet och göra den tillgänglig för Internetanvändare. Informationen skall vända sig till hushåll, små och medelstora företag och organisationer samt till

små och medelstora myndigheter. Det övergripande målet är att öka medvetenhet och kunskap om säkerhet på Internet för en säkrare användning, där man inte utsätter sig själv eller andra för onödiga risker. En särskild webbplats med interaktiv utbildning samt informationsmaterial finns sedan slutet av 2003. Under 2005 har också ett särskilt verktyg tagits fram för enskilda användare för att kunna genomföra säkerhetstest av den egna datorn.

Uppmärksammade erfarenheter av sårbarhet och risker i data- och kommunikationssystem har bidragit till att öka säkerhetsmedvetandet såväl i näringsliv och myndigheter som hos enskilda IT-användare. Även etiska frågeställningar och frågor om integritet har fått ökad uppmärksamhet. En rad åtgärder måste enligt utredningen vidtas för att förbättra säkerhetsmedvetandet och öka kunskaperna om informationssäkerhet. Det bör bland annat ske inom ramen för utbildningssystemet.

8.1.1 Grund- och gymnasieskolan

Det är lätt att lära sig och spännande att använda Internet, vilket gör att många barn och ungdomar använder tekniken i minst lika stor utsträckning som vuxna. Med detta följer flera risker. Barn inser inte på samma sätt som vuxna säkerhetsproblemen, utan öppnar till exempel gärna bifogade filer i e-post utan en tanke på att de kan innehålla skadlig kod. Barn har inte alltid omdöme att undvika olämpliga webbplatser och inte heller alltid förståelse för riskerna att lämna ut för mycket information om sig själv på egna webbsidor eller vid chattande. Det finns också en del ungdomar som har goda kunskaper i informationssäkerhet, men som av ungdomligt oförstånd och bristande uppfattning om etik och integritet använder kunskaperna till hackning och virusskapande.

Norska undersökningar visar dessutom att det man i allmänhet föreställer sig vara viktiga problem ur säkerhetssynpunkt för barn och ungdomar, i verkligheten långt ifrån alltid är de allvarligaste. Ett ökat säkerhetsmedvetande bör därför också syfta till en mera realistisk uppfattning av vad som utgör verkliga sårbarheter och problem.

Även om IT som sådant i dag är lätt att ta till sig, är säkerhet inte lika lätt att lära sig. Datoranvändning lär man sig ofta på egen hand, och säkerhet följer inte med någon automatik. Med tanke på att IT nu blivit en del av vardagen för de allra flesta, kanske redan från

förskoleåldern, både hemma och i skolmiljön, är det naturligt att skolan förmedlar kunskaper i informationssäkerhet som kan utveckla ett säkerhetsmedvetande, anpassat till respektive ålders behov och förutsättningar. Detta bör på ett tydligt sätt föras in i skolans läro- eller kursplaner på alla stadier.

Det finns starka skäl att öka insatserna för en bred påverkan av attityder till informations- och IT-säkerhet. Främst gäller det att öka medvetenheten om sårbarhet och risker, men också om metoder och åtgärder för en säkrare IT-användning. Utbildningen bör också förmedla att information kan vara en av ett hushålls, företags eller ett samhälles allra viktigaste tillgångar som måste kunna skyddas. Som enskilda individer måste vi också vara beredda att ta personligt ansvar för säkerhet upp till en viss nivå.

Utan säkerhetsmedvetande är flertalet åtgärder för att skapa en rimlig säkerhetsnivå av begränsat värde. Säkerhetsmedvetande bör därför byggas in redan i skolans grundläggande data- och IT-utbildning, både på grundskole- och gymnasienivå.

Bristande kunskaper såväl i pedagogisk IT-användning som i informationssäkerhet hos lärare är en kritisk faktor för att kunna förmedla etik och medvetande om behovet av säkerhet i IT-användningen. En av Stiftelsen för kunskaps- och kompetensutveckling (KK-stiftelsen) genomförd enkät under 2004 visar att en majoritet av lärarstudenterna är missnöjda med utbildningens IT-del, vilket leder till att pedagogiska verktyg används i låg grad. Även om det finns en allmän kompetens när det gäller datoranvändning som textbehandling och e-post så är dagens utbildning otillräcklig när det gäller att använda IT-verktyg i inlärningsprocessen.

Knappt hälften av lärarutbildarna använder IT-baserade läromedel i undervisningen. Det leder till att inte heller de blivande lärarna gör det. Om inte de blivande lärarna får kunskap i att hantera IT i utbildningen försenas utvecklingen mot att använda IT som ett kraftfullt pedagogiskt verktyg i skolan. Eleverna får då en stor del av sitt IT-kunnande på andra vägar än genom skolans undervisning. Frågor om etik och säkerhet riskerar härigenom få ett alltför begränsat utrymme i elevernas medvetande.

En klar majoritet av lärarna anser själva, enligt en enkät från KK-stiftelsen under 2005, att deras egen bristande kompetens är ett hinder för att använda IT i utbildningen. Samtidigt anser tre av fyra elever att användningen av IT i skolan ökar motivationen för skolarbetet. KK-stiftelsen satsar nu 100 miljoner på att stärka IT i

lärarutbildningen. Tillsammans med lärarutbildningar och satsningar inom kommuner och näringsliv beräknas insatsen överstiga 200 mkr under en tioårsperiod från och med 2005. Det är angeläget att satsningen även får en inriktning på säkerhetsmedvetande i IT-användningen.

I 1994 års läroplan för det obligatoriska skolväsendet, förskoleklassen och fritidshemmet (Lpo 94), framgår att rektor har ett ansvar för att ämnesövergripande kunskapsområden integreras i undervisningen i olika ämnen. Sådana kunskapsområden är exempelvis miljö, trafik, jämställdhet, konsumentfrågor, sex och samlevnad samt riskerna med tobak, alkohol och andra droger. Säkerhet och etik vid användning av datorer skulle med fördel kunna infogas i listan.

I gymnasieskolan ingår i dag datasäkerhet och kunskap om säkerhetsaspekter på bland annat Internet som ett moment i kursen Datorkunskap, som är gemensam i de flesta gymnasieprogram. Det finns också moment av informationssäkerhet i andra datakurser, framförallt inom den valbara kursen IT-samordning. Detta är i och för sig bra, men ser vi grund- och gymnasieskolan som en helhet finns åtminstone tre brister:

- Kunskap om säkerhetsproblem för att skapa säkerhetsmedvetande kommer in alltför sent i undervisningen. I gymnasiet har eleverna redan använt datorer och Internet i många år.
- Kunskap om informationssäkerhet tas i gymnasiet endast upp från ett tekniskt perspektiv. Det leder lätt till uppfattningen att säkerhet är något som tekniker ska leverera utan att andra ska behöva tänka på problemet.
- Användningen i skolan av IT-baserade läromedel och Internet är otillräcklig, delvis beroende på att många lärare saknar allmänkompetens för att använda IT som pedagogiskt hjälpmedel.

Konsekvensen blir bristande medvetenhet. Det finns även anledning att låta informationssäkerhet ur ett icke-tekniskt perspektiv vara en del av utbildningen i andra gymnasieämnen, till exempel inom företagsekonomi, handel, mediekommunikation och samhällskunskap. IT som pedagogiskt verktyg bör också få en mera framträdande plats i lärarutbildning och fortbildning av lärare.

8.1.2 Nationell informationssäkerhetskampanj

En nationell kampanj för säkerhet på Internet – Surfa lugnt – genomförs med start under våren 2005 i samverkan mellan ett femtontal statliga myndigheter, IT-branschens företag, Sveriges Kommuner och Landsting och andra organisationer. Kampanjen syftar till att öka medvetenheten om hur man kan skydda sig på nätet och hur man genom ett personligt ansvarstagande kan undvika att bli utnyttjad. Kampanjen vänder sig bland annat till ungdomar och småföretagare och uppmärksamheten kommer förhoppningsvis att bidra till ett ökat säkerhetsmedvetande.

8.2 Kvalificerad utbildning och forskning

8.2.1 Grundläggande utbildningsbehov

Dagens samhälle är beroende av IT och information. Den ökande förmågan att snabbt kommunicera stora och små datamängder med hjälp av elektroniska kommunikationer är en central funktion i globaliseringen. Informationstekniken krymper avstånd, höjer effektivitet och produktivitet i näringslivet och bidrar samtidigt till en ökad förståelse mellan olika kulturer och världsdelar. Allt under förutsättningen att vi kan lita på att systemen är robusta och informationen korrekt.

Utan tillgång till datorer och Internet kan företag och myndigheter inte bedriva stora delar av sin verksamhet. Medborgare kan inte få den information och utföra de många datorbaserade tjänster som man i dag är beroende av. Information är en av näringslivets och samhällets allra viktigaste tillgångar.

Medan det finns lång erfarenhet av att säkra fysiska tillgångar genom exempelvis byggnormer och trafiksäkerhet, har vi inte kommit särskilt långt i att säkra informationsflöden och IT-system. Även om informationen ofta är tillgänglig, korrekt och skyddad för obehörig insyn, behövs ett strukturerat sätt att arbeta med informationssäkerhet. Eftersom många system har nationell betydelse och är kritiska för samhällets funktionsförmåga, krävs också statlig kompetens inom området informationssäkerhet.

Dessvärre finns många exempel på när myndigheter inte har gjort rätt, vilket Försvarets radioanstalt (FRA) kunnat meddela respektive myndighet när man i samråd testat informationssäkerheten. Många samhällskritiska funktioner har allvarliga brister

i policy, regler, teknik och uppföljning. Till stor del beror det på att organisationer har tvingats skapa sin egen policy, rutiner och skyddsåtgärder på egen hand, ofta utan stöd av en välkänd och etablerad standard på området. Den dag skydd av information och IT blir lika naturlig som dagens skydd av fysiska tillgångar kommer samhällets risker på området att minska.

Några exempel på vad som har framkommit i testerna:

- En grupp inom en myndighet arbetade med ett känsligt projekt – så känsligt att gruppen såg sig nödgade att administrera sin Internetanslutning själva, helt utanför myndighetens ordinarie administration. Under tester i projektet ansåg gruppen att det var för krångligt att jobba med brandväggen, varför de ställde datorer utanför denna. En amerikansk organisation kontaktade senare myndigheten och meddelade att de utsattes för ett hackningsförsök som var spårat till denna. Efter kontroll av FRA visade det sig att hackare i flera omgångar hade tagit kontroll över datorer på myndigheten. Hackarna hade bland annat använt dessa för att ta kontroll över andra på Internet och för att installera s.k. underground chat-servrar. En av datorerna hade tidigare blivit infekterad av en mask. Den hade varit utan tillräckligt skydd mot Internet i ett år. Hela den lösning projektet använde har under senare tester visat sig klart undermålig. Med bättre teknik, rutiner, regelverk och framförallt medvetenhet hade detta inte inträffat. Kostnaderna för att städa upp efter misstagen var inte obetydliga. Myndighetens och Sveriges anseende inför den amerikanska organisationen har också lidit skada.
- Ett företag hade fått mycket känslig information stulen över Internet. Systemen hade hackats vid olika tillfällen och på olika sätt av en ytterst kompetent hackare. Denne har sannolikt försökt auktionera ut informationen till olika intressenter. Det som möjliggjorde för hackaren att stjäla informationen kan direkt härledas till den mänskliga faktorn. Trots att företaget kontinuerligt ser över sin policy och sitt regelverk räckte det att implementeringen på ett par ställen inte hade utförts i enlighet med dessa. Förlusten av den aktuella informationen skulle allvarligt ha äventyrat företagets verksamhet och renommé om det visat sig att hackaren agerat på någon illasinnad aktörs uppdrag eller på annat sätt spridit vidare den olovligt åtkomna informationen. Sådana omständigheter

framkom inte i detta fall. Företaget som upptäckte intrånget i systemen, tog i ett tidigt utredningsskede kontakt med polisen. Frånvaron av internationella och effektiva spårningsmekanismer runt Internet – legala såväl som praktiska – medförde att utredningstiden blev mycket lång, över två år, och resurskrävande för både polis och målsägande.

- En myndighet hade inom en sexmånadersperiod utsatts för åtminstone två kvalificerade trojan-attacker. Man kunde konstatera att förövaren hade kommit över mycket sekretesskänsliga dokument. Även i detta fall kan de utnyttjade tekniska bristerna direkt härledas till bristfälliga policyn och rutiner som, i den mån de existerade, inte var kända av dem som berördes. Medvetenheten har varit låg, vilket till del beror på att nyckelpersoner i ledande position haft en ovilja att se behovet av informationssäkerhet. Den konstaterade förlusten av information har orsakat mycket stor skada för myndigheten och för Sverige.
- På en myndighets webbserver upptäcktes en mask med en installerad bakdörr. Denna kunde konstateras ha varit aktiv i två år utan upptäckt, trots att masken var av ett primitivt slag. Antalet personer som obehörigen har varit inne på denna server är troligtvis mycket stort, kanske tusentals. Detta kunde hända därför att myndigheten saknade virusvarningssystem och inte heller hade rutiner och regler för till exempel hur man ska sätta upp en webbserver. Skadan för myndigheten och Sverige är omöjlig att uppskatta då det inte går att veta vilka som varit inne på servern och inte heller vad dessa gjort eller vilka dokument de kommit över.

De redovisade exemplen är endast ett urval av brister som framkommit i den kvalitetshöjande testverksamheten. De visar både på behov av en höjd utbildningsnivå inom området informationssäkerhet, och behov av att använda kvalitetsmetoder vid säkringen av informationssystem.

En stor del av utbildningen i informationssäkerhet och IT-säkerhet sker genom enskilda företag som utbildningsanordnare och via konsultinsatser i anslutning till utvecklingen av nya system och produkter inom IT-området. Det sker främst i form av fortbildning, men till betydande del även som grundläggande utbild-

ning. Utbudet av dessa utbildningar är omfattande. De uppdateras kontinuerligt och är i praktiken en del av IT-utvecklingen.

En betydande del av utbildningsbehovet måste tillgodoses inom högskolans ram. Liksom inom högskolan i övrigt, måste inom området informationssäkerhet kopplingen stärkas mellan utbildning och forskning. Utbildningen skall vila på vetenskaplig grund, liksom på beprövad erfarenhet. Ett viktigt tillämpningsområde för forskningen inom informationssäkerhetsområdet måste vara som utgångspunkt för den utbildning som bedrivs i kompetenshöjande syfte. Det gäller både för kortare eller mera grundläggande utbildningar och för mera specialinriktade utbildningar som förbereder för fortsatt forskning eller kvalificerad verksamhet inom området informationssäkerhet.

Informationssäkerhet måste i dagens samhälle utgöra en baskunskap för många yrkesgrupper – alltifrån jurister, samhällsvetare och ekonomer till tekniker. En nödvändig förutsättning för ett bra innehåll och kvalitet i utbildningen är att det finns en tillräcklig kår av högstadielärare som även är aktiva forskare inom området.

Jurister behöver definiera vilken information som är nödvändig för att en organisation skall kunna uppfylla sina legala skyldigheter. En särskild svårighet finns i mötet mellan juridiken och tekniken. I den privata sektorn blir detta tydligt vid upprättandet av avtal. Inom den offentliga sektorn visar sig svårigheterna också vid utredning och lagföring av brott. Inom rättsväsendet finns ett stort behov av kompetens på informationssäkerhetsområdet, inte minst när det gäller polis och åklagare. I domstolarna är det åklagarens uppgift att åskådliggöra brottet och de element som ingått i den brottsliga handlingen. De bevis som åberopas är ofta tekniskt komplicerade och den koppling mellan den åtalade och brottet som beviset skall styrka är inte alltid uppenbar för den som saknar särskilda kunskaper på området.

Institutet för rättsinformatik (IRI) är en forskningsavdelning vid Stockholms universitets juridiska fakultet. Viktiga delar av verksamheten omfattar informationssäkerhetsfrågor. I den juridiska grundutbildningen tas dessa frågor upp redan under första studieåret och återfinns senare såväl på magisternivå som på doktorandnivå.

För dataingenjörer och systemvetare borde det vara självklart att IT-säkerhet ingår i utbildningen. Men det är viktigt att inte begränsa sig till IT-säkerhet, utan även ha en förmåga att sätta in det i det större sammanhanget, informationssäkerhet. I flera

utbildningar, till exempel inom ekonomi, juridik och samhällsvetenskap borde som en del i utbildningen kunna ingå att analysera ett fiktivt företag eller en myndighet och göra en informationssäkerhetsanalys med avseende på vilka de kritiska informationstillgångarna är. Hur skyddas tillgångarna? Vilken policy och vilka rutiner bör skapas? IT-säkerhet är en del av skyddet, men endast en del.

Samhällsvetare behöver analysera vilken information som oundgängligen måste kunna flöda inom ett samhälle. Ekonomer kan beräkna vad tillgång till information kan betyda i produktivitet och i ekonomiskt hänseende. De kan också omsätta vad förlust av information kan betyda i ekonomiska termer och utifrån detta beräkna skyddsbehovet. Tekniker kan sedan utifrån de analyser som andra yrkeskategorier presenterar, ta fram teknik som gör det möjligt att hantera information på det önskade sättet.

I dag hanterar tekniker ofta informationssäkerhet utan tillräcklig förankring i sin organisations aktuella behov. Tekniker får ofta på egen hand lösa balansen mellan å ena sidan tillräckligt god informationssäkerhet och å andra sidan effektivitet och smidighet i de valda lösningarna. I den mån de har förankrat denna balans i sin organisation, vilar dessvärre ofta förankringen inte på någon genomtänkt policy baserad på organisationens faktiska behov.

Generellt kan sägas att de utbildningar som är vanliga hos personer i högre ledande befattningar i såväl offentlig som privat verksamhet, bör innehålla en del av grundläggande informationssäkerhet. Som framgår av exemplen på funna brister, hade dessa kunnat undvikas om ledningen hade haft högre medvetenhet och kunskap i informationssäkerhet. Om Sverige vill fortsätta sin strävan att vara en ledande IT-nation, måste det anses vara en prioriterad åtgärd att höja medvetenheten och kunskapen i myndigheters och företags ledningar.

Det finns mot denna bakgrund skäl att etablera en frivillig men rekommenderad grundläggande kurs i informationssäkerhet på 3–5 poäng inom utbildningarna till civilingenjör, civilekonom, jurist och samhällsvetare. Man bör också överväga att ha en motsvarande kurs i efterutbildningen av läkare. För systemvetare och dataingenjörer bör en sådan kurs vara obligatorisk med möjlighet till ytterligare fördjupning på ca 5 poäng.

I dag finns utbildningsprogram och fristående kurser på högskolenivå inom området. En kartläggning av utbildning inriktad mot samhällets krisberedskap på högskolor och universitet i

Sverige har under 2004 genomförts av Krisberedskapsmyndigheten. Resultatet anger att inom området Informationssäkerhet finns fem utbildningsprogram och ett tjugofemtal fristående kurser med inriktning mot krisberedskap. De har ett intag på totalt drygt 650 platser per år. Det finns ytterligare program och fristående kurser inom området, huvudsakligen med mera teknisk inriktning.

Som ett exempel kan nämnas Chalmers i Göteborg, vars institution för Data och IT har ca 200 anställda, inklusive doktorander. Institutionens två grundutbildningar är D- respektive IT-linjerna. D-linjen är djupare och mera teknisk, medan IT-linjen har större bredd. De valfria kurserna gör att skillnaden mellan utbildningarna i praktiken inte blir så stor.

En av de valfria kurserna som institutionen ger är 3 poäng Datasäkerhet. Denna kurs kan läsas även av studenter på andra program, som elektroteknik, eller av studenter på IT-universitetet. Kursen har en tyngdpunkt på IT-säkerhet, men berör även standarder i viss mån. De mjuka (programorienterade) delarna i kursen är problematiska. Dels är det svårt att finna aktuell och relevant kurslitteratur, dels kan det vara svårt att motivera teknologer att intressera sig för icke-tekniska aspekter. Från institutionen är man positiv till att föra in fler element om standarder, bland annat Ledningssystem för informationssäkerhet (LIS). Från och med nästa år samlas alla IT-säkerhetskurser till en fördjupningsinriktning – *Security*.

Bland programmen kan nämnas Datateknik, nätverk och säkerhet, 120 poäng vid KTH, IT-säkerhet 120 poäng vid Blekinge Tekniska Högskola, Nätverk och datasäkerhet 120 poäng vid Växjö Universitet och Tillförlitliga datorsystem 60 poäng påbyggnad vid Göteborgs universitet.

Vid Blekinge Tekniska högskola finns även en vidareutbildning för yrkesverksamma. Utbildningen är en kompetenshöjande vidareutbildning inom IT-säkerhet och går på halvfart under två år. Personal från Rikskriminalpolisen, Säkerhetspolisen och Polishögskolan har deltagit vid planeringen av utbildningen.

8.2.2 Magisterutbildning

Det finns också ett magisterprogram i Security engineering på 60 poäng vid Blekinge Tekniska Högskola. Den har inriktning på IT-säkerhet och delvis på IT-forensisk (kriminalteknisk) verksamhet.

Chalmers grundutbildningar kan i dag byggas på med en ettårig mastersutbildning. Institutionen för data- och IT erbjuder kursen Tillförlitliga datorsystem (*Dependable Computer Systems*, DCS). I denna ingår obligatoriskt 4 poäng datasäkerhet.

Från och med 2007 är det tänkt att Chalmers utbildningssystem ska ha anpassat sig enligt Bolognadeklarationen, som syftar till att likforma de europeiska utbildningssystemen för att främja rörlighet, öka anställningsbarhet och öka Europas attraktivitet som utbildningskontinent.

Modellen innebär i stora drag 3 års grundutbildning, 2 års masterutbildning och 3 års doktorandutbildning. Konsekvensen för Chalmers blir att ett år av grundutbildningen flyttar till mastersutbildningen. DCS-programmet blir alltså tvåårigt och kommer att ingå i det normala utbildningsprogrammet. Förslaget till nytt mastersprogram kommer att behandlas under våren 2005. Enligt vad utredningen erfarit kommer den nya mastersutbildningen att få tydligare inslag av informationssäkerhet.

Bilden från andra universitet och högskolor varierar en del från Chalmersexemplet. Den kommer sannolikt att bli mera likartad, i takt med att Bolognamodellen får genomslag i utbildningsorganisationen. Gemensamt är dock att helhetssynen på informationssäkerhet, och utbildningen om standarder, till exempel Ledningssystem för informationssäkerhet behöver förstärkas, även i utbildningar som fördjupar delar av informationssäkerhetsområdet, tekniskt eller i annat avseende. Problemet med relevant kurslitteratur är också generellt för informationssäkerhet. Det beror delvis på den snabba utvecklingen inom området, delvis på att informationssäkerhetsfrågornas betydelse behöver öka även inom universitets- och högskoleområdet.

Behovet av kvalificerad utbildning i informationssäkerhet ökar bland annat i takt med det växande behovet att kunna rekrytera personer till ledande befattningar inom näringsliv och förvaltningar. På senare år har alltfler företag, efter internationell förebild, börjat använda uttrycken CIO eller CISO, *Chief Information Officer respektive Chief Information Security Officer* (närmast

Informationssäkerhetschef eller -direktör), som titel på den högste ansvarige inom informationssäkerhet. En informationssäkerhetschef ingår i företagets ledningsgrupp och svarar för såväl administrativ som teknisk informationssäkerhet samt ansvarar normalt också för utarbetandet av ett företags policy inom området och genomförandet av policyn.

Ytterst innebär uppgiften ett ansvar för att analysera vilken information som är central för organisationen liksom att avgöra vilken IT-plattform som är lämplig för att hantera organisationens information. Den ansvarige skall också säkra informationen inom policy, regelverk och tekniska lösningar. Det är sannolikt att CIO kommer att bli en allt vanligare yrkesgrupp inom såväl näringsliv som myndigheter. Genom att den blir en vanligare yrkesgrupp i samhället kan medvetenheten för informationssäkerhet och kvaliteten i insatsen stärkas.

Det finns därför skäl att stimulera till etablering av CIO-utbildningar eller motsvarande inom ramen för högskoleutbildningen av ekonomer och ingenjörer. Utbildningsbehovet kan naturligtvis variera mellan olika företag och olika myndigheter. Generellt kan dock konstateras att det finns behov av CIO-utbildning på magisternivå (mastersnivå) med minst 40 poängs påbyggnad utöver akademisk grundexamen.

Omfattningen i antal utbildningsplatser, profilering och placering av en sådan utbildning bör bli föremål för ytterligare bedömningar. Initiativ kan tas av enskilda universitet och högskolor, som kan erbjuda en kvalificerad nivå.

Krisberedskapsmyndigheten, som har ett sammanhållande myndighetsansvar inom krishanteringsområdet, bör tillsammans med ansvariga myndigheter inom utbildningsområdet ha ett utpekat ansvar för att tillse att behovet av högre utbildning inom informationssäkerhetsområdet tillgodoses.

8.2.3 Forskning

De växande behoven av säkra informationssystem ställer krav på ökade resurser för forskning om informationssäkerhet. Det gäller såväl grundforskning, och forskning om tillämpade metoder och ledningssystem, programvara och produkter. En betydande del av dagens forskning bedrivs i gränszonen mellan ren forskning och utvecklingsinsatser i IT-företagen.

Eftersom det kommersiella värdet av utvecklingen av IT-teknologin är så betydande, är detta ganska naturligt. Samhället i form av internationella organisationer, Europeiska unionen och staten kan och bör dock ställa krav på säkerhet eller säkerhetsnivåer som måste uppnås i utvecklingen av nya systemlösningar. Marknaden ställer också allt högre krav på säkra system och säkra lösningar.

Forskning behövs även för att utveckla kompetens och stimulera kvalitet i utbildningen. Krisberedskapsmyndigheten har ett särskilt ansvar inom forskningsområdet för att stimulera, initiera och delvis även finansiera forskning inom området informationssäkerhet. Det gäller både för forskning inom det allmänna universitets- och högskoleområdet och inom ramen för Försvarshögskolans och Totalförsvarets forskningsinstituts verksamhet. Detta ansvar behöver förtydligas ytterligare.

Att säkra rikets ledning och tillgången till samhällskritisk infrastruktur ställer stora krav på säkerhet i informationshanteringen. Utan en hög nivå på den nationella informationssäkerheten ökar också riskerna för svåra påfrestningar i det fredstida samhället. Staten måste därför vara beredd att engagera sig i att bygga upp en forskarkompetens inom området informationssäkerhet.

För att utveckla kunskap och kompetens inom ett delvis nytt ämnesområde som informationssäkerhet behöver forskning initieras, stimuleras och följas upp. Det är viktigt att utifrån en god överblick och bedömningsförmåga inrikta forskningen mot nydanande mångvetenskapliga perspektiv, som på sikt kan ge praktisk nytta inom det aktuella området. Forskningsbaserad kunskap bygger på långsiktighet och uthållighet i projektsatsningar och i kompetensutveckling bland berörda forskare.

För att kunna avtappa för forskningsområdet nödvändig analytisk förmåga, bland annat som ett stöd för utbildningar inom området, bör investeringar göras över flera år i framväxt av kreativa och internationellt konkurrenskraftiga forskningsmiljöer. Mångfald bland utförare är en grundläggande förutsättning för en dynamisk ämnesutveckling. Ett visst risktagande är dessutom ofrånkomligt i all nydanande forskningsfinansiering, även om man skapar processer i uppbyggnaden som syftar till att begränsa riskerna.

8.2.4 Krisberedskapsmyndigheten

Krisberedskapsmyndigheten (KBM) har sedan den etablerades genomfört tematiska utlysningar av fleråriga forskningsmedel kring områdena Hot och hotutveckling samt kring Sårbarhet och krisberedskap på lokal och regional nivå. Totalt har satsningen legat på ca 12 milj. kr. per år med ett högt söktryck. Samråd har förevarit med statens sex samverkansområden. Projekten har diskuterats i KBM:s vetenskapliga råd. För närvarande sker en satsning på ett tredje insatsområde, forskning kring Terrorism och terroristbekämpning. Insatserna kommer sannolikt att förankras också i en internationell forskarmiljö.

På motsvarande sätt borde staten genom den roll som Krisberedskapsmyndigheten har i forskningshänseende utveckla ett tematiskt område kring Informationssäkerhet. Ett första steg skulle kunna vara att engagera en grupp av forskare för att inom relevanta ämnen ta fram kunskapsöversikter. Det gäller bland annat att sätta svenska ämnesbidrag i ett internationellt sammanhang, då forskningsfronten på detta område till stora delar ligger bortom landets gränser.

Den överblick och den förmåga till syntes av flera olika ämnesdelar som krävs för en sådan uppgift innebär att en inledande fas borde anförtros ledande forskare med gedigen vetenskaplig meritering. Syftet är inte att möjliggöra för någon enskild forskare att lyfta fram sin speciella vinkel på ett ämne i vardande. Från ett helhetsperspektiv kan flera forskare täcka in rådande kunskapsläge, samt inte minst peka på viktiga kunskapsluckor.

Flera sådana översikter torde kunna ge en balanserad och heltäckande bild av hur ett nytt forskningsområde skulle kunna utvecklas vidare samt vilka embryon till forskningsmiljöer man skulle kunna bygga på i en fortsatt satsning.

Sådana översikter kommer sannolikt att visa på att en hel del forskning inom området redan bedrivs inom landet och internationellt, men i isolerade öar i ganska specialiserade ämnesgrupperingar. Genom en första kunskapsöversikt kan man kartlägga hur dessa potentiella bidragsgivare till ämnesutvecklingen borde kunna knytas samman och därmed komplettera varandra inom ett nationellt program för informationssäkerhet. En sådan profilhöjning inom kompetenssfären blir även ett slagkraftigt instrument i det internationella erfarenhets- och myndighetsutbytet inom ämnesområdet.

Ett nästa steg vore att behandla dessa kunskapsöversikter vid konferenser med tungt internationellt inslag. Svenska forskare engageras för att i det vetenskapliga samtalet med internationella kollegor hävda sina perspektiv och lyfta fram sina speciella nischer inom den internationella ämnesutvecklingen. Även företrädare för det praktiska genomförandet inom området Informationssäkerhet bör medverka aktivt vid sådana inventerande konferenser. Praktiker inom området besitter värdefulla insikter som kompletterar de forskningsbaserade kunskaper som forskarna tar fram.

Ett ämnes utveckling främjas av att kunna förena forskningsbaserade kunskaper med erfarenhetsbaserade insikter. Behovsmotiverad forskning syftar ytterst till att lösa olika praktiska, framtida uppgifter, inte minst inom kompetensutveckling och kompetensförsörjning. Därför är också närvaron av personer med praktisk erfarenhet värdefull.

Förhoppningsvis stimulerar konferenser, som bygger på utförda kunskapsöversikter, flera svenska forskargrupper att engagera sig inom det nya ämnesområdet. Inte minst värdefullt vore att kunna rekrytera yngre, lovande forskare genom postdoktorala karriärmöjligheter.

Om ett antal sådana forskare kunde stimuleras att ägna sin forskarkraft åt detta ämnesområde i vardande, i stället för att inriktas mot mer traditionella, disciplinorienterade frågeställningar vid redan etablerade miljöer, kunde området ges en kreativ, nydanande impuls och på sikt generera värdefulla kunskapsbidrag. Så har skett inom andra ämnesområden.

Efter genomförda konferenser kan arbetsmöten eller seminarier ordnas med intresserade forskare och utvalda praktiker för att värdera hur ett vetenskapligt förankrat ämnesområde skulle kunna stimuleras och utvecklas i Sverige. I sammanhanget måste också värderas hur denna forskning kan kopplas till existerande och framtida internationellt ledande forskning inom området. Vilka speciella svenska nischområden som kan profileras behöver också värderas. Hur denna forskning kan kopplas till existerande eller framtida utbildningar och fortbildning behöver klarläggas.

Hur forskningen kan och bör leverera användbar kunskap till avnämare behöver diskuteras ingående. Likaväl som forskare måste inse praktikens dagliga villkor, behövs också en bättre förståelse för forskningens villkor och för den forskningsbaserade kunskapens möjligheter och begränsningar.

Finns det ett intresse bland forskare och relevanta myndighetsföreträdare att gemensamt utveckla det nya ämnesområdet bör man initiera projekt med enskilda forskare och forskargrupper att i konkurrens söka forskningsmedel. För att en satsning skall uppfattas som meningsfull inom vetenskapssamhället bör den årliga ramen vara 10–15 miljoner SEK. En budgetram i den storleksordningen skulle ge utrymme för två till tre fleråriga programsatsningar. Kriterier för prioriteringar bland de sökande måste fastställas inför en utlysning av forskningsmedlen. Vetenskaplig kvalitet samt relevans för ämnesområdet bör vara grundläggande, då man vill främja utvecklingen av forskning inom ett nytt mångvetenskapligt ämnesområde med en tydlig praktikerorientering.

Forskargrupper som erhåller bidrag måste kunna förlita sig på att satsningen är flerårig. Uthållighet är en nödvändig förutsättning för långsiktigt verkande kunskapstillskott. Det är en kvalitativ aspekt som också är väsentlig för att inom landet skapa kompetens och personliga förmågor att slagkraftigt samverka internationellt inom ämnesområdet. Dels behöver svenska forskare i konkurrens ta hem forskningsanslag från till exempel EU:s forskningsprogram, dels behöver man kunna erbjuda utländska kollegor specialkunskaper i utbyte mot deras nischkompetens. En viktig del i den initiala finansieringen av de svenska forskargrupperna blir således att de är medel också för medverkan i olika internationella sammanhang.

Avtappning av resultat från forskargrupperna till den dagliga praktiken kan endast förväntas på sikt. Däremot kan utbildningsprogram, kurser och seminarier som bygger på den finansierade forskningen komma igång relativt snart. Genom referensgrupper, dialoger och liknande bör kunskapsförmedlingen kunna främjas tidigt. Forskare är även pedagoger och bör förväntas delge sina kunskapsrön i olika former. Förnyelsen av kompetens och generationsskiften inom forskarkåren kan också säkras genom koppling till utbildande institutioner.

Inom informationssäkerhetsområdet finns stora utbildningsbehov. Dessa nya program för kompetensförsörjning och utveckling bör vila på vetenskaplig grund och inte enbart baseras på insikter, som erfarna praktiker kan förmedla genom sina personliga upplevelser.

8.2.5 Försvarshögskolan

Försvarshögskolan (FHS), är en civil myndighet, vars uppgift är att bidra till nationell och internationell säkerhet genom forskning och utbildning. Forskningen bedrivs inom delvis unika kunskapsområden och sprids därefter vidare till övriga samhället och även utanför Sveriges gränser.

Försvarshögskolan utbildar militära och civila ledare, nationellt och internationellt, vilka skall bidra till att hantera dagens och morgondagens krissituationer och säkerhetsproblem. Högskolan kan inom området informationssäkerhet bidra med stöd vid studieverksamhet samt ge analysstöd i nära samverkan med andra berörda statliga aktörer – exempelvis Regeringskansliet och Krisberedskapsmyndighetens Informationssäkerhetsråd.

Försvarshögskolan bedriver på uppdrag av såväl militära som civila myndigheter och Regeringskansliet bland annat forskning och studier genom sitt Centrum för Asymmetriska Hot och Terrorismstudier (CATS). Vid försvarshögskolan utvecklas även Informationsoperationer som ett akademiskt ämne i internationell samverkan med bland annat University of St. Andrews i Skottland och National Defense University i USA. Aktuella delområden är informationsterrorism, policy och skydd av nationell infrastruktur på informationsområdet, varseblivningsanalys och psykologiska operationer samt metodik för omvärldsanalys.

Institutet för högre totalförsvarsutbildning, IHT, som ingår i FHS, utbildar ledande befattningshavare i frågor av stor betydelse för informationssäkerhet, bland annat vid den årliga Solbackakursen för högre chefer inom förvaltning, näringsliv och medier samt för regering och riksdag.

Försvarshögskolans arbete präglas av säkerhetspolitiskt fokus med tvärsektoriellt arbetssätt och är kopplat till såväl militär som civil, statsvetenskaplig, teknisk, polisiär och folkrättslig kompetens. Forskning och studier rör olika aspekter av informationsoperationer i fred, kris och krig med allt från informationsattacker till nätverksattacker. Även informationsoperationer som drabbar näringslivet studeras i ett särskilt projekt.

Asymmetriska hot från icke-statliga aktörer studeras i nära samverkan med internationella forskningscentra om terrorism. Försvarshögskolan anordnar även kvalificerade seminarier rörande såväl tekniska, folkrättsliga som underrättelseorienterade fråge-

ställningar. Försvarshögskolan har dock inget operativt ansvar inom området informationsoperationer.

Försvarshögskolan, med sina flervetenskapliga utbildningar och forskningsprogram, har förutsättningar att genomföra utbildning inom området informationssäkerhet. Flera av högskolans samarbetspartners har väl utvecklade program inom informationssäkerhet.

FHS administrerar i dag studerande från Försvarsmakten som deltar vid nationella och internationella högskolor och universitet. Nationellt sker detta främst inom ramen för Försvarsmaktens doktorandprogram och internationellt som studerande i kvalificerade utbildningsprogram. De utländska skolornas utbildningsprogram kan till viss del användas som förebild för svenska liknande utbildningar. FHS samarbete med nationella högskolor och universitet kan därför bidra till att utveckla en svensk informationssäkerhetsutbildning.

En utbildning i informationssäkerhet skulle kunna ske med en praktisk inriktning för certifiering av nyckelpersonal inom myndigheter och företag, samt med en teoretisk magisterutbildning för fördjupade kunskaper inom området. Utbildningen bör kunna genomföras både under en koncentrerad utbildningstid och fördelad under ett antal år. Försvarshögskolans redan befintliga kompetens för utbildning och forskning inom ledarskap, management, krishantering och teknik gör att högskolan har flera av de förutsättningar som krävs för att genomföra en magisterutbildning inom informationssäkerhet.

8.2.6 Totalförsvarets forskningsinstitut

Totalförsvarets forskningsinstitut (FOI) har till uppgift att bedriva forskning, metod- och teknikutveckling samt utredningsarbete för totalförsvaret och som stöd för nedrustning och internationell säkerhet.

Av förordningen (2003:131) om försvarsunderrättelseverksamhet framgår att forskningsinstitutet skall bedriva försvarsunderrättelseverksamhet. Uppgiften skall fullgöras genom analyser av information som inhämtats från offentliga informationskällor eller som lämnats av uppdragsgivare.

Totalförsvarets forskningsinstitut skall följa utvecklingen inom sitt ansvarsområde och bygga upp kunskaper och kompetens för att tillgodose framtida behov och verka för att försvarsforskningen

nyttiggörs även utanför totalförsvaret. Myndigheten skall särskilt verka för samverkan mellan militär och civil, respektive mellan nationell och internationell forskning.

Myndigheten är till åttio procent uppdragsfinansierad, vilket innebär att den forskning som bedrivs till betydande del styrs av kundernas behov. Uppdragsgivare är bland annat Försvarsdepartementet, Utrikesdepartementet, Försvarsmakten, Krisberedskapsmyndigheten och Försvarets materielverk.

Vid avdelningen för försvarsanalys genomförs studier och forskning inom området informationssäkerhet på olika systemnivåer. Uppdragen har bland annat varit orienterade mot säkerhetspolitiska bedömningar, hotbildsanalyser, framtidsstudier och samhällsorienterade sårbarhetsanalyser. Verksamheten har även omfattat systemnära säkerhetsanalyser och scenarion av IT-system inom till exempel vattenförsörjning, telekommunikation, elproduktion och drivmedelsförsörjning. Under senare år har kunskapsutveckling skett inom området säkring av viktig infrastruktur, där bland annat frågor om informationssäkerhet får en alltmer framträdande roll. Denna forskning har finansierats av Krisberedskapsmyndigheten.

Vid avdelningen för ledningssystem har institutionen för systemanalys och IT-säkerhet byggt upp verksamhet och kompetens inom framförallt den tekniska delen av IT-säkerhetsområdet.

Forskningen inom IT-säkerhet har tre huvudinriktningar: offensiv inriktning, defensiv inriktning samt design av säkerhetsarkitektur. Den största finansiären av forskningen har hittills varit Försvarsmakten men civila uppdragsgivare har även förekommit. Utöver forskning bedrivs utbildning rörande IT-säkerhet inom Försvarsmakten.

En viktig resurs vid avdelningen för ledningssystem är IT-säkerhetslaboratoriet. Laboratoriet är uppbyggt med hög flexibilitet för att lätt kunna konfigureras om för att simulera nya system och egenskaper.

8.2.7 Sics och andra forskningsinstitut

Forskning inom informationssäkerhetsområdet bedrivs även inom andra organisationer. The Swedish Institute of Computer Science, Sics, är ett icke vinstdrivande forskningsinstitut med ett hundratal forskare från hela IT-området, med projekt bland annat inom framtida Internet-teknologi och interaktionen mellan människa

och dator. Forskningen bedrivs i nära samverkan med industrin och det internationella forskarsamhället. Sics har i internationella bedömningar rankats bland de främsta forskningsinstituten i världen.

Sics ägs till tre fjärdedelar av svensk industri och en fjärdedel av staten, genom Föreningen för Datateknisk forskning och SITI, Svenska IT-institutet. Målet är att bidra till konkurrensförmågan hos svensk industri genom att bedriva avancerad forskning inom strategiskt viktiga områden av datavetenskap och aktivt främja användningen av nya idéer och resultat i industrin och samhället i stort. Sics har inte primärt fokus mot informationssäkerhet, men en stor del av forskningen berör i praktiken frågor om funktionalitet och säkerhet.

Sics finansiering sker förutom med medel från industrin också från Vinnova och Stiftelsen för strategisk forskning. Institutet deltar i en rad EU-finansierade forskningsprojekt.

Vid sidan av Sics finns även andra forskningsorgan inom IT-området som Viktoria-institutet i Göteborg, Santa Anna-institutet i Linköping och Interaktiva institutet som bedriver verksamhet på flera platser i Sverige. De bildar tillsammans SITI, Svenska IT-Institutet AB.

Utredningen har betonat vikten av samarbete mellan offentlig och privat sektor. Sics fyller tillsammans med övriga institut en mycket viktig funktion för att vara en avancerad brygga mellan näringslivets forskningsbehov, statens behov av att främja forskningen och forskarvärlden inom IT-området. Utredningen anser att institutens forskning borde få en förstärkt inriktning på projekt inom området informationssäkerhet.

8.2.8 Europeiska forskningsinsatser

EU initierar och finansierar en omfattande forskning inom informationsteknikens område. Informationssamhällets teknik (IST) är ett delområde inom EU:s sjätte ramforskningsprogram med en budget på drygt 3.600 miljoner euro under fyra år. Det finns fyra huvudprioriteringar inom IST. De gäller för det första tillämpad forskning avseende informationssamhällets teknik som berör samhälleliga och ekonomiska utmaningar. För det andra gäller det teknik för kommunikation, hantering av information och programvara. För det tredje gäller det komponenter och mikrosystem. Det fjärde

området gäller teknik för kunskapshantering och intelligenta gränssnitt.

Främst det första området berör informationssäkerhetsfrågor. Antalet projekt är mycket stort.

Den förändrade synen på säkerhet efter de uppmärksammade terrordåden i början av 2000-talet och Unionens allt högre säkerhets- och försvarspolitiska profil ledde till ett kommissionsbeslut om en *Preparatory Action on Security Research* (PASR). I praktiken är detta ett förberedande forskningsprogram om ca 65 miljoner euro under tre år som syftar till forskning till stöd för fredsfrämjande insatser, Petersbergsinsatser, det vill säga insatser under andra pelaren. Programmet i sin slutliga utformning har en bredare ansats på säkerhet. I de projekt som skall bedrivas ingår bland annat ”Optimerad säkerhet i och skydd av nätverkssystem” samt ”Kompatibla och integrerade informations- och kommunikationssystem”.

PASR har genomfört en första ansökningsomgång. Kommissionen har också givit ut ett meddelande om fortsättningen för PASR där bland annat kommissionen säger sig vilja tillskapa ”en rådgivande styrelse” för säkerhetsforskningsprogrammet med representanter för såväl industri, forskningsorganisationer och användare. Denna skall ha en rådgivande roll avseende PASR innehåll och genomförande. Dessutom avser kommissionen att inleda en ”interinstitutionell diskussion” om ett framtida säkerhetsforskningsprogram.

Kommissionen betonade i meddelandet också att behoven emanerade från säkerhetsstrategin, den gemensamma utrikes- och säkerhetspolitiken (GUSP), den gemensamma säkerhets- och försvarspolitiken (ESFP) och kommissionsinitiativ relaterade till Europeiska unionens interna säkerhet, skall beaktas i utvecklingen av PASR.

Joint Research Centre (JRC) är ett generaldirektorat inom kommissionen som bedriver uppdragsforskning, tillhandahåller vetenskapliga råd och teknisk kunskap samt genomför annan verksamhet till stöd för Kommissionens policyskapande generaldirektorat. JRC som består av sju olika institut, arbetar med ett vitt spektrum av frågor. Ett institut inom JRC är *Institute for the Protection and the Security of the Citizen*, beläget i Ispra, Italien, vid vilket det bedrivs ett program för *Cyber Security*. Forskningen inom detta område berör bland annat ”Digitala identiteter” och ”Interdependens och risk i informationsinfrastrukturen”. Denna

forskning är finansierad genom ett så kallat ”specifikt program” inom sjätte ramforskningsprogrammet.

Sverige bör ha har en hög ambition i att delta såväl i EU:s policyskapande arbete för att inrikta forskningen inom informationssäkerhetsområdet och som avnämare och genomförare av större forskningsprojekt inom området. Det är en angelägen uppgift både för Regeringskansliet och myndigheter som Krisberedskapsmyndigheten och Vinnova, liksom för svenskt näringsliv, att delta i arbetet och få del av de betydande forskningsresurser som EU kommer att satsa under kommande år inom informationssäkerhetsområdet. Till ambitionerna bör också höra att utveckla samarbete med partners i andra länder eftersom EU-finansierade forskningsprojekt ofta förutsätter samverkan mellan aktörer i flera medlemsländer.

8.3 Kryptologisk kompetens

En väsentlig delmängd av informationssäkerhet är kommunikationssäkerhet och det närbesläktade begreppet signalskydd. Traditionellt har signalskydd varit en militär angelägenhet, där det gällt att skydda sin egen kommunikation mot fientlig signalspaning.

Två komponenter i signalskyddet är trafikskydd och textskydd. Trafikskydd går ut på att förhindra eller försvåra för utomstående att uppfatta kommunikationen. Det kan man göra till exempel genom att välja andra sambandsmedel än radio eller genom att ofta byta radiofrekvens, om möjligt flera gånger i sekunden. Textskydd går ut på att se till att utomstående inte kan förstå innehållet i kommunikationen även om de lyckas uppfatta den. Detta sker genom att man krypterar innehållet.

Kryptering har länge varit en avancerad disciplin, som kräver mycket hög kompetens, främst inom matematik. Denna kompetens har behövts inom såväl signalskydd som signalspaning. Även om vissa komponenter som språklig kompetens har haft viss betydelse, så har traditionellt sett matematik ändå varit den helt dominerande komponenten inom kryptokompetens. I dag ser bilden annorlunda ut, men inte beroende på att matematiken minskar i betydelse. Tvärtom används alltmer avancerad matematik inom modern kryptering.

Men till skillnad mot tidigare krävs även hög kompetens inom data. Skälet härtill är naturligtvis att kryptering oftast utförs på datorer. Med detta följer en ny sårbarhet. Hur vet man att det är rätt program som exekveras? Lägger krypteringsprogrammet någon kopia av klartexten på olämpligt ställe? Är den underliggande slumptalsgeneratorn korrekt skriven? Att ta reda på svaret på dessa och många andra frågor utifrån kanske enbart ett komplicerat dataprogram kräver hög kompetens.

Med IT-revolutionen har kryptering blivit en angelägenhet långt utanför det militära området. De som behöver kommunikationssäkerhet finner vi i dag överallt i samhället. Rättsväsendet kommer att ha ett växande behov av tillgång till kryptologisk kompetens för den brottsutredande verksamheten.

Finansiella transaktioner och anbud vid upphandlingar sker i dag via Internet. IT ger också användaren möjligheter att kryptera kommunikation och hårddiskar utan att egentligen ha någon teknisk kompetens på området. Talar man i en GSM-telefon krypteras ljudet mellan basstationen och telefonen. Det finns program för automatisk kryptering av hårddiskar, vilket förhindrar förlust av information om datorn blir stulen. I trådlösa nätverk kan administratören välja att använda kryptering för att minska risken att någon utomstående i närheten obehörigen tar sig in i nätverket. Trådlösa tangentbord kan kommunicera krypterat med datorn för att minska risken för avlyssning. Inget av detta märker användaren, men krypteringen finns där ändå som säkerhetsåtgärd.

Kombinationen IT och krypto ger också möjlighet att signera dokument, så att mottagaren kan vara förvissad om att dokumentet inte är förfalskat eller förvanskat och att det är skrivet av den som utger sig för att vara avsändare. De flesta vanliga e-postprogram stöder denna funktionalitet. Det finns även många andra nya användningsområden. Men om man behöver en hög säkerhetsnivå räcker det inte med att förlita sig på allt för enkla kryptolösningar eller varianter som kan laddas ner från Internet. Framför allt gäller det att välja en säkerhetsnivå som är anpassad efter den egna verksamhetens behov.

Behovet av kryptokompetens i samhället är alltså stort och växande. Kompetenskraven har höjts kraftigt under senare år.

Standardiseringen på informationssäkerhetsområdet har i dag, som tidigare redovisats under avsnittet 7.8 kommit mycket långt. De internationella standardiseringsorganen har till sitt förfogande

experter inom varje relevant delområde inom informationssäkerhet, inklusive kryptologiområdet.

Bland standarder och utvecklingsprojekt för standarder inom SC 27 ISO/IEC kan nämnas:

- SIS LIS-projekt (Ledningssystem för informationssäkerhet)
- Common Criteria för evaluering och certifiering
- Standarder för kryptologiska algoritmer och protokoll

Näringsliv och myndigheter måste ha hög kompetens vad gäller datasäkerhet. Däremot är det inte alltid nödvändigt att man har egna kryptologer. För större företag med forsknings- och utvecklingsavdelningar med ambitioner att vara världsledande och kunna licensiera ut tekniker är det motiverat, men dessa företag är få till antalet. Förhoppningsvis blir de fler i framtiden.

Ur kompetenssynpunkt räcker det dock inte med några få personer med hög kompetens inom kryptologi. Det krävs så många att man skapar en kritisk massa för kompetensutveckling. Samhällets kritiska infrastruktur behöver dessutom tillgång till kryptologer på samma sätt som i TSA:s (Totalförsvarets signalskyddssamordning) roll för totalförsvaret.

För att stimulera tillväxten av särskild kompetens för samhället och de större företagen kan man exempelvis sponsra eller finansiera doktorandtjänster vid universiteten. Ytterligare en aspekt är tillgången till inhemska leverantörer, hur den kan främjas. Det är en fördel att kunna använda inhemska leverantörer som kan tillhandahålla källkod för utvärdering.

8.4 Kontroll och rådgivning enligt säkerhetsskyddslagen

Säkerhetspolisen och Försvarsmakten ansvarar för att kontrollera säkerhetsskyddet inom sina respektive ansvarsområden. Vid alla kontroller ingår informationssäkerhet som en naturlig del. Säkerhetspolisen bedriver också en omfattande rådgivningsverksamhet gentemot statliga myndigheter, landsting, kommuner samt enskilda, som omfattas av säkerhetsskyddslagen. Även i rådgivningsverksamheten är frågor om informationssäkerhet vanligt förekommande.

Enligt Säkerhetspolisens och Försvarsmaktens erfarenheter är de kontroller som genomförs med stöd av säkerhetsskyddslagen ofta

av stor betydelse för att uppmärksamma och åtgärda brister i säkerhetsskyddet. De bidrar också till att medvetandegöra ledningarna i de berörda kontrollerade organisationerna om behovet av tillfredsställande skydd, bland annat på informationssäkerhetsområdet. Det är vanligt att man vid kontrollerna uppmärksammar brister till exempel i hur man hanterar datorer (både fristående datorer och nätverk), telefonväxlar, mobiltelefoner och mobila datorer. Ofta saknas styrdokument avseende informationssäkerheten och personalen har otillräcklig utbildning om IT-säkerhet.

Som exempel kan nämnas kontroller av två olika myndigheter, vilka bedriver samhällsviktig verksamhet. I båda fallen upptäcktes att information som var hemlig med hänsyn till rikets säkerhet hanterades tillsammans med öppen information i myndigheternas interna nätverk. Penetrationstester, som Försvarets radioanstalt utförde som en del av kontrollen, visade att det fanns ett flertal brister i informationssäkerheten. Bristerna innebar bland annat att myndigheternas interna nätverk var sårbara för obehöriga intrång och attacker via Internet.

Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd har nyligen reformerats. I dessa ingår allmänna bestämmelser om informationssäkerhet, krav på krypto, regler för hantering av kryptonycklar och signalskyddsmaterial mm. Särskilda regler finns för informationssäkerhet för hemliga uppgifter i IT-system med avseende på bland annat intrångsskydd, skadlig kod, intrångsdetektering, säkerhetsloggning och hantering av digitala lagringsmedier.

8.5 Beställar- och leverantörskompetens

8.5.1 Beställarkompetens

Samhället har låg beställarkompetens för informationssäkerhet, vilket utgör ett grundläggande problem. Ägarna av samhällskritisk infrastruktur måste först inse att den infrastruktur de äger är kritisk, att den behöver skyddas, samt att det inte enbart behövs ett fysiskt skydd, utan även ett informationssäkerhetsskydd.

Ökade krav från statens sida vid upphandling kan också förväntas öka förutsättningarna för svensk IT-industri att kunna

leverera säkra produkter och system och därvid även stärka sin konkurrensförmåga på den internationella marknaden.

Behov av beställarkompetens hos ägare av kritisk infrastruktur kan generaliseras till ägare av information i samhället i största allmänhet, alltså inte enbart kritisk infrastruktur. Varje myndighet måste kontinuerligt varje år göra en risk- och sårbarhetsanalys som inbegriper den för myndigheten kritiska informationen. Det finns behov av att utveckla kompetensen i både risk- och sårbarhetsanalys och i själva riskhanteringsprocessen. Motsvarande gäller även för kommuner och landsting och inom näringslivet.

Även myndigheter, näringsliv och andra aktörer som inte hanterar samhällskritisk infrastruktur uppvisar ofta brister i beställarkompetens för informationssäkerhet. Det kan bero på bristande medvetenhet, brist på genomtänkt policy, avsaknad av kvalitetssäkring enligt Ledningssystem för informationssäkerhet eller andra skäl. Det förekommer inte sällan att övriga krav på funktionalitet specificeras före och under upphandling medan kraven på funktionalitet för informationssäkerhet specificeras i efterhand.

Det är ofta förenat med betydande kostnader att i efterhand korrigera kraven på informationssäkerhet vid upphandling. Ibland blir dessutom måluppfyllelsen otillräcklig. När beställaren däremot är medveten om vad som krävs för ett bra informationssäkerhetsskydd, är det också möjligt att definiera skyddet, anpassa det och upphandla.

Tillgång till certifierade produkter enligt Evalueringskriterier för IT-säkerhet, *Common Criteria*, (ISO/IEC IS 15408) eller för tjänster enligt Ledningssystem för informationssäkerhet, LIS, (SS-ISO/IEC 17799, SS 627799-2) skulle avsevärt underlätta upphandling av informationssäkerhet. Utveckling av informationssäkerhet med stöd av internationellt accepterade standarder är en konstruktiv metod för att skapa tillit och förtroende såväl inom en organisation som mellan olika parter. Den möjliggör också en meningsfull revision av säkerheten, eftersom revisionen kan ske gentemot definierade mål och kvalitetsrutiner.

Common Criteria behandlar kravspecifikation, granskning och evaluering av teknisk IT-säkerhet för produkter och system. LIS rymmer för verksamheter och tjänsteproduktion liknande funktioner i ett bredare perspektiv, som innefattar såväl administrativa som tekniska kvalitetskrav på informationssäkerheten.

Staten har ett ansvar för att utveckla beställarkompetensen. Det kan bland annat ske genom att successivt infoga kravet på certifiering vid upphandling men också genom tillämpning av kvalitetskraven i Ledningssystem för informationssäkerhet, LIS eller varianten OffLIS. Statskontoret bör ha ett särskilt ansvar för att stimulera en sådan ambitionshöjning i statens krav på säkra produkter och kvalitativa tjänster vid upphandling.

Det krävs också en satsning på fortbildning i upphandlingsteknik inom området informationssäkerhet, som en del i en integrerad kravspecifikation vid upphandling. Expertmedverkan i form av konsultinsatser vid upphandling av komplexa informationssystem kan vara motiverad.

Sannolikt kommer en ökad beställarkompetens att generera en större efterfrågan som marknaden snabbt kommer att reagera på och söka tillfredsställa. De värden som finns investerade i näringslivets nät, och som måste skyddas, innebär dessutom att det finns ytterligare starka drivkrafter för att utveckla kompetensen. Näringslivets behov av kompetensförsörjning har därför också betydelse för utformningen av den nationella strategin.

Företeelsen outsourcing, det vill säga att lägga ut viktiga delar av verksamheten på lång entrepenadförvaltning ökar kraftigt behovet av beställarkompetens. Här kommer också tidsaspekten in som en viktig faktor. Vid första tillfället kan finnas en hög kompetens för att upphandla och sluta ett avtal om outsourcing av till exempel IT-funktioner. Efter fem år eller längre tid utan medarbetare med adekvat kompetens riskerar man hamna i ett underläge vid förnyad eller förlängd upphandling. Här bör för statens del Statskontoret ha ett särskilt ansvar för att kunna bistå med erfarenheter, kompetens och stöd. Även i sådana fall kan finnas skäl för expertmedverkan genom konsultinsatser. Frågeställningen har stor giltighet även för kommuner och landsting.

För många aktörer, till exempel mindre och medelstora företag eller enskilda kommuner, kan outsourcing samtidigt vara ett effektivt medel för att etablera funktionalitet med en kompetens och kvalitet som man saknar möjlighet att utveckla i egen regi. Outsourcing ställer dock alltid stora krav på beställarkompetensen.

Krisberedskapsmyndigheten definierar i sina rekommendationer en basnivå för IT-säkerhet, BITS, som minst måste uppnås för IT-system, det vill säga som bedöms nödvändiga för att upprätthålla en organisations normala verksamhet även under fredstida kriser.

Om denna basnivå är tillräcklig skall avgöras genom risk- och sårbarhetsanalys i varje enskilt fall.

BITS har fyllt en funktion, dels genom sin existens, dels genom att etablera principen om en lägsta godtagbara nivå. Arbetet pågår nu för att få BITS att konvergera mot informationssäkerhetsstandard LIS eller OffLIS i de delar där parallellitet finns.

Denna utveckling kommer att höja ambitionsnivån i statens krav på informationssäkerhet i offentliga system, på liknande sätt som sker i ett antal med för Sverige jämförbara länder. Informationssäkerhet måste omfatta såväl tekniska system som administrativa rutiner. En ökad användning av internationellt accepterade standarder kommer att påskynda utvecklingen mot säkra informationssystem i hela samhället.

Särskild uppmärksamhet bör dessutom ägnas kompetensen i avtalsfrågor. Mötet mellan teknik och juridik, särskilt när det gäller informationssäkerhet är komplicerat. Även här bör Statskontoret ha ett utvecklingsansvar.

8.5.2 Leverantörskompetens

Den offentliga verksamheten måste ta tillvara den säkerhetskompetens och den snabba utveckling som sker inom det privata näringslivet. Det är inte en uppgift för den offentliga sektorn att tillgodose behovet av leverantörskompetens utan det bör främst ske genom det utbud som utvecklas på den privata marknaden.

Först i den mån marknaden inte är tillräckligt stor eller av någon annan anledning olämplig, måste staten kunna gå in. När det gäller infrastruktur och informationssystem som är nationellt samhällskritiska, kan det hävdas att staten har ett ansvar. I allmänhet har dock staten möjlighet att stimulera leverantörskompetens genom teknikupphandling på marknaden, som inrymmer också utvecklingsinsatser. Men staten kommer varken ha anledning eller möjlighet att själv i någon större omfattning stå för denna kompetens.

Staten kan därför anses ha ett ansvar att skapa förutsättningar för en hög kompetensnivå inom de företag som medverkar till att tillgodose samhällets behov av informationssäkerhet.

8.6 Revision och certifiering

Vid 2000-säkringen i samband med millennieskiftet visades att revision är en konstruktiv metod för säkerhetsgranskning och säkerhetsutveckling också inom området IT-säkerhet. Revisionsområdet för näringslivet med Föreningen Auktoriserade revisorer (FAR) och Riksrevisionen för statliga myndigheter, liksom internrevisionen inom många myndigheter ägnar i dag frågor om informationssäkerhet en större uppmärksamhet i såväl effektivitetsrevision som i den årliga revisionen.

För FAR gäller bland annat en ny redovisningsstandard RS 401, Revision i en datoriserad informationssystemmiljö, sedan 2004. RS 401 överensstämmer med den internationella redovisningsstandarden ISA 401. Syftet med denna revisionsstandard är att lägga fast standarder och ge vägledning när revision utförs i en datoriserad informationssystemmiljö. Revisorn skall skaffa sig förståelse för systemfunktionerna, deras innebörd och komplexitet samt vilken tillgång de ger till uppgifter som skall användas i revisionen.

Revisorn skall också skaffa sig förståelse för hur klientens verksamheter inom den datoriserade informationssystemmiljön är organiserade och i vilken utsträckning databehandlingen sker centralt eller utspritt i företaget samt hur tillgänglig informationen är. Reglerna är utarbetade bland annat efter erfarenheter från de uppmärksammade stora redovisningsskandalerna i amerikanska företag. Reglerna fokuserar mera på IT-säkerheten i redovisningssystemen än på informationssäkerhet i dess bredare betydelse och kan behöva kompletteras.

Inom Riksrevisionen pågår ett projekt som omfattar såväl effektivitetsrevisionen som den årliga revisionen som syftar till att utveckla och fördjupa revision av informationssäkerhet. Nya regler beräknas kunna tillämpas från och med 2007. Projektarbetet bedrivs utifrån en bredare syn på informationssäkerhet. Utredningen anser det angeläget att projektarbetet kan bedrivas skyndsamt så att nya regler för revision av tillfredsställande informationssäkerhet inte onödigtvis försenas.

Tillämpning av standarder, till exempel LIS, Ledningssystem för informationssäkerhet, i ett företags eller myndighets verksamhet underlättar för såväl intern som extern revision. Då finns klara förutsättningar från de krav som standarden ställer, såväl

administrativt som tekniskt, att revidera mot. Saknas tillämpning av standarder försvåras en effektiv revision.

Att underlätta för en effektiv revision av informationssäkerhet är ett centralt motiv för utredningens starka förord för att tillämpa standarder i myndigheter och i annan verksamhet i kommuner och landsting liksom i näringslivet.

Revision av informationssäkerhet kräver ofta medverkan av specialister inom området informationssäkerhet. Tester av informationssäkerhet i myndigheter, till exempel penetrations- och funktionstester som Försvarets radioanstalt genomför genom sin teknikkompetensfunktion bidrar till att ge underlag för förbättringar i myndigheternas tillämpning av informationssäkerhet. Utredningen understryker dock att sådana tester bör ske i samråd med myndigheternas ledningar för att ge bästa resultat i uppföljningen av resultaten.

Certifiering av informationssäkerhet är möjlig. Utredningen har dock valt att inte föreslå ett generellt krav på certifiering. Det är omfattande, kan vara tidsödande och kostnadskrävande även om resultatet, en certifiering enligt standard, i sig kan vara angelägen.

Att samhället erbjuder möjligheten att certifiera sig på frivillig väg bör däremot uppmuntras. Redan i dag är det i Sverige genom en svensk ordning, möjligt att certifiera ett ledningssystem för informationssäkerhet mot standarden SS 62 77 99 – 2. I Tyskland har utvecklats en modell med tre olika former av certifiering i stigande grad, två självcertifieringsnivåer och en formell certifiering. Varje certifieringsnivå innebär att flera av skyddsåtgärderna i en standard måste implementeras och tillämpas. Syftet är att organisationen skall vinna en högre grad av tillit vid varje nivå.

Självcertifiering innebär att organisationen själv förklarar sig uppfylla kraven i de två inledande nivåerna. Den som anser sig uppfylla basnivåerna respektive tilläggskraven kan låta sig listas på BSI:s (*Bundesamt fur Sicherheit in der Informationstechnik*; den tyska myndigheten för informationssäkerhet) webbplats. Den högsta nivån är en formell certifiering, som utförs av oberoende IT-revisor och certifikatet utfärdas av BSI, som därmed utfäster att organisationen uppfyllt de för nivån nödvändiga kraven.

Utredningen anser att den modellen med en stegvis höjning av ambitionsnivån i riktning mot certifiering har fördelar. Den medverkar till att underhålla ett högt säkerhetsmedvetande och stimulerar till aktiva egna insatser för berörda att höja ambitionerna

vid en tillämpning av informationssäkerhetsstandard. Utredningen avser återkomma till frågan i sitt organisatoriska betänkande.

8.7 Fortbildning och erfarenhetsåterföring

Området informationssäkerhet, liksom IT-säkerhet, befinner sig i mycket snabb förändring. Den teknik och de metoder som används, liksom de risker och hot mot säkerheten som uppstår förändras oupphörligt, när varje teknikgeneration i princip byts ut under en tre- till femårsperiod. Även möjligheterna att komma tillrätta med sårbarheter och risker förändras snabbt. Det gör att behovet av fortbildning i frågor som rör informationssäkerhet är mycket omfattande.

Varje myndighet, företag, kommun, landsting eller annan organisation har ett ansvar för att se till att adekvat fortbildning genomförs för alla medarbetare, som har uppgifter inom området informationssäkerhet. I många fall handlar det om kvalificerade fortlöpande utbildningsbehov. Det kan gälla bland annat utbildning i risk- och sårbarhetsanalys liksom utbildning i själva riskhanteringsprocessen.

Tillämpning av informationssäkerhetsstandard som LIS och OffLIS ger en god grund för de utbildningsinsatser som är nödvändiga på informationssäkerhetsområdet. SIS, Swedish Standards Institute, ger ut handböcker och genomför utbildning i tillämpningen av informationssäkerhetsstandard. SIS är en medlemsbaserad förening, ett centrum för arbetet med standarder och samarbetspartner med de europeiska och globala nätverken, European Committee for Standardization, CEN, och International Organization for Standardization, ISO.

Beställarkompetensen måste utvecklas genom fortbildning i frågor om kravspecifikation, upphandling och avtalsrätt. I andra fall kan det röra sig om bredare fortbildning med tonvikt på säkerhetsmedvetande.

Inte minst då informationsfunktioner och IT-funktioner läggs på entreprenad kan behovet av fortbildning för den egna personalen vara betydande.

Erfarenheter från säkerhetsarbete, sårbarhetsanalys och krishantering måste återföras i en kompetenshöjande fortbildning inom främst myndigheter och företag med ansvar för samhällskritisk infrastruktur.

Informationssäkerhet är alltid en ledningsfråga. Fortbildningsbehovet gäller därför även den verkställande nivån och styrelsenivån i myndigheter och företag.

8.8 Signalspaningskunskap som skydd för IT-system

På liknande sätt som Sverige har kunnat ta tillvara signalspaningens unika kompetens för att skydda svenska kryptosystem bör man kunna ta tillvara även den kunskap om brister i IT-säkerhet som utvecklats inom signalspaningen. Det har betydelse för möjligheten att skydda samhällsviktiga system mot kvalificerade IT-relaterade hot.

Före IT-revolutionen var huvudfrågan för staten att skydda samhällets kritiska kommunikationer (regeringen, försvarsmakten etc.) från andra länders signalspaning. Efterhand breddades verksamheten till att även omfatta andra samhällsviktiga sektorer som till exempel bankväsendet. När vi i dag talar om informationssäkerhet som det övergripande begreppet, omfattar det såväl IT-säkerhet som signalspaning och administrativ säkerhet. Det är en konsekvens av att samhällsviktiga IT-system finns inom alltfler områden.

Hotet mot informationssystemen har under de senaste åren fått allt större offentlig uppmärksamhet. Det som främst diskuteras är de nya sårbarheter som uppstått i och med informationsteknologins införande i till exempel el- och telesystemen och de ömsesidiga beroendeförhållanden som följt av detta. Vad som är mindre känt är de hot som uppstår genom att allt fler stater lägger alltmer resurser på underrättelseinhämtning (offensiv förmåga) via det globala nätet.

Varje dag rapporteras nya virus eller olika typer av gränsöverskridande kriminell verksamhet via de globala informationsnäten. Mörkertalet är stort och långt ifrån allt blir känt och publikt. Säkerhetspolisen anger i sin öppna verksamhetsrapport för 2003 att man har uppmärksammat att ett stort antal aktörer fortsätter visa ökat intresse och förmåga att genomföra olika typer av IT-relaterade angrepp.

Andra studier visar tydligt på sårbarheten inför angrepp från främmande länders underrättelsetjänster och liknande kvalificerade aktörer. Mot dessa har enskilda, företag och organisationer mycket svårt att värja sig. Även teleoperatörer och andra aktörer med hög

teknisk kompetens har svårt att värja sig mot denna typ av aktiviteter, trots att det många gånger är deras system som utnyttjas. En rad rapporter från svenska myndigheter[1] och samhällssektorer förstärker intrycket av att staten måste ta ett större ansvar för att möta de kvalificerade IT-relaterade hoten. Detta konstaterade också utredningen i sin andra delrapport (sid. 27):

Utredningen vill peka på att det finns kvalificerade IT-relaterade hot som med den framväxande globala kommunikationsstrukturen och den nya IT-tekniken i en förlängning också skulle kunna innebära ett hot mot rikets säkerhet. Dessa hot utgör självfallet också ett hot mot många andra verksamhetsområden. Var gränsen går mellan allmänna hot och hot mot rikets säkerhet är inte absolut.

Ett av de främsta medlen, förutom det förebyggande arbetet, för att möta de kvalificerade IT-relaterade hoten är att i högre grad inrikta vår underrättelsetjänst emot dem. Detta understryks också i regeringens hittillsvarande strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system (prop. 2001/02:1 sid. 103):

För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas.

Signalspaningen har stor betydelse för möjligheterna till skydd emot kvalificerade aktörsbundna IT-relaterade hot. Hittills vidtagna åtgärder för att öka säkerheten i IT-systemen kommer inte att vara tillräckliga för att skydda oss från aktörsstyrda kvalificerade IT-relaterade hot av säkerhetspolitisk dignitet. Signalunderrättelsetjänsten har en unik möjlighet att med sin kompetens kartlägga och identifiera illasinnade aktörer, och därmed bidra till att avvärja denna typ av hot.

En av orsakerna till detta är att de flesta åtgärder för att öka säkerheten och robustheten i samhällsviktiga IT-system utgår ifrån olika typer av icke-aktörsbundna störningar, till exempel elavbrott, eller skydd emot relativt sett mindre kvalificerade aktörer, som till exempel hackers eller spridare av datavirus. Denna typ av åtgärder är långt ifrån tillräckliga när det handlar om nationella underrättelsetjänster, terrornätverk eller annan grov och organiserad internationell kriminalitet, som använder det globala nätet för sina syften.

[1] Se till exempel Krisberedskapsmyndighetens årliga hot och riskrapport, Totalförsvarets forskningsinstituts användarrapport, En studie om det kvalificerade IT-hotet (FOI-R-1182-SE) i februari 2004

I sådana fall krävs att underrättelse- och säkerhetstjänsten, i första hand signalspaningen, har direktiv och mandat att agera mot hoten. Härigenom kan ett trovärdigt nationellt cyberförsvar upprätthållas, som även kan hantera kvalificerade attacker från olika aktörer. Detta förhållande har bland annat framhållits av FRA-utredningen (SOU 2003:30, sid. 85):

Utredningen vill i dessa sammanhang peka på att i omvärlden prioriteras signalspaningsorganens verksamhet till skydd för IT-system mycket högt. Signalspaningsorganens möjligheter att spela en avgörande roll för skyddet mot kvalificerade IT-relaterade hot bedöms i dessa sammanhang som stora.

I Sverige har signalspaning och signalskydd legat långt framme genom tidigare satsningar på olika informationssäkerhetsrelaterade områden (kryptologisk kompetens, IT-skyddsförmåga m.m.)

Kryptoforcering och signalskydd

Svensk signalspaning har traditionellt haft en mycket god kunskap i konsten att forcera kryptoskydd av olika slag. Inom signalspaningen finns en hög kompetens vad gäller kryptologisk/matematisk analys och dessutom en ”organiskt nedärvd” metodologisk och institutionell förmåga att forcera kryptosystem. Allt detta förutsätter dock att signalspaningen förmår att dra till sig en kritisk massa av kompetenta individer och erbjuda en miljö som främjar det kreativa tänkande som denna hårt specialiserade och avancerade gren av tillämpad matematik kräver.

Den största gruppen disputerade matematiker utanför universitetsvärlden finns vid Försvarets radioanstalt. En förutsättning för att kunna rekrytera kompetenta matematiker är att de får arbeta med de bästa tänkbara arbetsredskapen. I dessa sammanhang handlar det om beräkningskraft, vilken Försvarets radioanstalt kontinuerligt uppgraderar genom inköp av nya stordatorer. Detta har tidigare skett med 3–4 års intervall under de senaste årtiondena. Den senaste uppgraderingen skedde 2001, vilken endast var en mindre uppgradering, och nästa är planerad först till 2007/08.

Konstruktion och test av egna kryptosystem för att skydda landets information och forcering av kryptosystem är två sidor av samma mynt. För att kunna konstruera säkra system som bedöms kunna stå emot forcering av utländska organisationer med stora resurser krävs att ständigt själv söka forcera och analysera nya

komplicerade kryptosystem. Dessa två sidor kräver samma kompetens och det är av avgörande betydelse att de genomförs integrerat, inom samma organisation eller på annat sätt under starkt samordnade former.

För att hålla jämna steg med den snabba tekniska utvecklingen är det nödvändigt att hela tiden ha tillgång till största möjliga beräkningskraft i form av mycket snabba datorer. Nya datorers beräkningskraft fördubblas i princip var 18:e månad. Det är endast en av flera faktorer som påverkar förmågan. De nya säkerhetshoten, i form av terrorism och grov avancerad och organiserad brottslighet, utnyttjar det globala nätet samt en alltmera tillgänglig och ständigt mera avancerad kryptoteknik för sin verksamhet. Därmed ökar också förekomsten – volymen – av krypterade meddelanden, eftersom alltfler aktörer söker dölja sin information.

Utöver att Sveriges och Europas säkerhet riskerar att försämras, innebär volymökningen även att den egna forceringsverksamheten, som syftar till att förbättra de egna kryptosystemen, hela tiden måste ta mindre tid. Det betyder i sin tur att den egna beräkningskraften kontinuerligt måste öka. Takten är i dag för låg, vilket kan försvaga förmågan.

När det gäller kryptologisk kompetens och förmåga har Sverige under lång tid haft en framträdande plats i Europa. Det har betydelse för såväl Sveriges inflytande på området i Europa som för svensk krypto- och kommunikationsindustri. Den successivt, i förhållande till det ständigt växande behovet, försvagade beräkningskraften riskerar att påverka Sveriges samlade kompetens på området och därigenom ställningen i Europa. Mest allvarligt är emellertid att den svenska informationssäkerheten riskerar att försämras.

Den pågående omstruktureringen av Försvarsmakten och de medföljande neddragningarna inom dess stödmyndigheter påverkar även Försvarets radioanstalt. Under perioden 2005-09 kommer resursbristen att drabba den nationella informationssäkerheten om inte frågan om finansiering av en nödvändig uppgradering av beräkningskraft kan lösas.

För att tillvarata den kryptologiska kompetensen i signalskyddssammanhang bildades 1981 den s.k. kryptologpoolen mellan Försvarets radioanstalt och dåvarande Totalförsvarets signalskyddsavdelning (TSA) vid Försvarsmakten. Avsikten var att tillvarata den känsliga kunskap om angreppssätt som Försvarets radioanstalt i sin forceringsverksamhet kunnat utveckla för att

skydda svenska kryptosystem mot motsvarande angreppssätt från omvärlden.

Det förtroende som etablerats genom en organisatorisk koppling och arbetsrotation har varit en förutsättning för överföringen av känslig signalspaningsinformation till den säkerhetsorienterade verksamheten vid TSA.

Inom framför allt den tekniska informationssäkerheten har ett liknande förhållande som inom kryptoforcering och signalskyddet börjat växa fram, det vill säga en tydlig koppling mellan signalspaningsförmåga och förmågan att skydda egna system.

Som framgår av tidigare resonemang har signalspaning en mycket central roll såväl för offensiv förmåga (underrättelseinhämtning) som för *defensiv* förmåga (signalskydd och IT-säkerhet) vilket inte alltid framgår av den offentliga debatten då verksamheten omgärdas med mycket hög sekretess. Den offensiva aspekten är avgörande för den defensiva förmågan, på samma sätt som kryptoforceringen är för det traditionella signalskyddet.

Utvecklingen av den svenska signalspaningen med relevans för detta område hänger nära samman med de satsningar som har genomförts under de senaste decennierna för att ta del av den ökade trafiken mellan datorer. Syftet har framförallt varit att skapa ett bättre strategiskt underrättelseunderlag för att stödja till exempel svenska internationella insatser, bekämpningen av terrorism och övriga transnationella hot. En positiv bieffekt av denna kunskap är att den har visat sig kunna ge en unik möjlighet till ett ökat skydd mot de mera teknikspecifika IT-relaterade hoten.

Vad det här handlar om är att signalspaningen först och främst kan ge underrättelser avseende hot och aktörer som agerar mot svenska informationssystem. Men en minst lika viktig del är den kunskap om brister i olika tekniska informationssystem, som erhålls i den egna underrättelseverksamheten genom signalspaning. Denna kunskap måste, på samma sätt som forceringskunskapen nyttjas för signalskyddet, kunna användas till skydd för samhällsviktiga system.

8.9 Utredningens slutsatser om kompetensfrågor

Säkerhetsmedvetandet har under de senaste åren höjts i näringsliv och myndigheter liksom hos enskilda IT-användare. En rad åtgärder måste dock, enligt utredningen, vidtas för att ytterligare

förbättra säkerhetsmedvetandet och öka kunskaperna om informationssäkerhet. Det bör bland annat ske inom ramen för utbildningssystemet. Lärarutbildningarna måste utvecklas så att kunskap om och förståelse för IT- utvecklingen i samhället blir obligatorisk. Särskilt med fokus på de möjligheter och problem som finns kring IT i skolan, både som läromedel men även som administrativt hjälpmedel och redskap för kommunikation.

Säkerhetsmedvetande, anpassat till respektive ålders behov och förutsättningar, måste byggas in i skolans grundläggande data- och IT-utbildning i såväl grund- som gymnasieskolan.

En betydande del av utbildningsbehovet måste tillgodoses inom högskolans ram. Kopplingen måste stärkas mellan utbildning och forskning. Informationssäkerhet bör utgöra en baskunskap för många yrkesgrupper, alltifrån jurister, samhällsvetare, lärare och ekonomer till tekniker. Utredningen förordar att frivilliga men rekommenderade kurser i informationssäkerhet på 3–5 poäng införs i bland annat utbildningarna till civilingenjör, civilekonom, jurist och samhällsvetare, samt motsvarande i efterutbildningen av läkare. För systemvetare och dataingenjörer bör en sådan kurs vara obligatorisk med möjlighet till ytterligare fördjupning.

På senare år har alltfler företag inrättat funktioner som informationssäkerhetschef. Motsvarande behov av ansvariga tjänster finns inom myndighetsvärlden. Utredningen anser att det finns skäl att stimulera till etablering av kvalificerad utbildning i informationssäkerhet på magisternivå för att bland annat tillgodose efterfrågan av tjänster inom området. Sådan magisterutbildning planeras enligt vad utredningen erfarit bland annat starta vid Chalmers i Göteborg. Magisterutbildning med inriktning mot det kriminaltekniska området bedrivs vid Blekinge Tekniska Högskola.

Forskning

De växande behoven av säkra informationssystem ställer krav på ökade resurser för forskning inom informationssäkerhet. Krisberedskapsmyndigheten har ett särskilt ansvar inom forskningsområdet för att stimulera, initiera och delvis även finansiera forskning inom området informationssäkerhet. Det gäller både för forskning inom det allmänna universitets- och högskoleområdet och inom ramen för Försvarshögskolans och Totalförsvarets

forskningsinstituts verksamhet. Detta ansvar behöver förtydligas ytterligare.

Att säkra rikets ledning och tillgången till samhällsviktig infrastruktur ställer stora krav på säkerhet i informationshanteringen. Staten måste därför vara beredd att engagera sig i att bygga upp en forskarkompetens inom området informationssäkerhet. Forskningsbaserad kunskap bygger på långsiktighet och uthållighet i projektsatsningar och i kompetensutveckling bland berörda forskare. Mångfald bland utförare är en grundläggande förutsättning för en dynamisk kunskapsutveckling.

Krisberedskapsmyndigheten bör utveckla ett tematiskt område kring informationssäkerhet. Forskargrupper som erhåller anslag skall veta att satsningen är flerårig.

Försvarshögskolans samarbete med nationella högskolor och universitet kan bidra till att utveckla utbildningen inom informationssäkerhet. En utbildning i informationssäkerhet skulle kunna ske med en praktisk inriktning för certifiering av nyckelpersonal inom myndigheter och företag.

Totalförsvarets forskningsinstitut skall verka för samordning mellan militär och civil, respektive mellan nationell och internationell forskning. Vid avdelningen för försvarsanalys bedrivs studier och forskning inom området informationssäkerhet på olika systemnivåer. Under senare år har kunskapsutveckling skett inom området säkring av viktig infrastruktur, där bland annat frågor om informationssäkerhet får en alltmer framträdande roll. Forskningen inom IT-säkerhet har tre huvudinriktningar: offensiv inriktning, defensiv inriktning och design av säkerhetsarkitektur.

Utredningen har betonat vikten av samarbete mellan offentlig och privat sektor. Sics fyller tillsammans med övriga institut en mycket viktig funktion för att vara en avancerad brygga mellan näringslivets forskningsbehov, statens behov av att främja forskningen och forskarvärlden inom IT-området. Utredningen anser att institutens forskning borde få en inriktning på projekt inom området informationssäkerhet

Europeiska unionen

EU initierar och finansierar en omfattande forskning inom informationsteknikens område. Förberedelserna för det sjunde utvidgade ramforskningsprogrammet har nu påbörjats. Informa-

tionssamhällets teknik (IST) inom det sjätte ramforskningsprogrammet har haft en budget på 3.600 miljoner euro under fyra år. Inom IST finns fyra huvudprioriteringar: för det första informationssamhällets teknik som berör samhälleliga och ekonomiska utmaningar, för det andra teknik för kommunikation, hantering av information och programvara, för det tredje komponenter och mikrosystem och för det fjärde teknik för kunskapshantering och intelligenta gränssnitt. Främst det första området berör informationssäkerhet. Antalet projekt är mycket stort.

Förebyggande insatser i säkerhetsforskning (Preparatory Action on Security Research, PASR) är ett förberedande forskningsprogram under tre år. Det har i sin slutliga utformning fått en bred ansats på säkerhet. I projekten som bedrivs ingår bland annat ”Optimerad säkerhet i och skydd av nätverkssystem” samt ”Kompatibla och integrerade informations- och kommunikationssystem”.

Joint research Centre (JRC) är ett generaldirektorat inom Kommissionen som bedriver uppdragsforskning m.m. JRC består av sju olika institut. Inom ramen för dessa bedrivs bland annat program på temat *Cyber Security*. Forskningen om programmet berör bland annat ”Digitala identiteter” och ”Interdependens och risk i informationsinfrastrukturen”.

Sverige bör ha en hög ambition att delta såväl i EU:s policyskapande arbete för att inrikta forskningen inom informationssäkerhetsområdet och som genomförare av större forskningsprojekt inom området. Det är en angelägen uppgift både för Regeringskansliet och myndigheter som Krisberedskapsmyndigheten och Vinnova liksom för svenskt näringsliv och högskole- och universitetsvärlden att delta i arbetet och få del av de betydande forskningsresurser som EU kommer att satsa under kommande år inom området informationssäkerhet. Det kräver också ett utvecklat samarbete med partners i andra EU-länder.

Kryptologisk kompetens

Kryptering har länge varit en avancerad disciplin, som kräver mycket hög kompetens. Till skillnad från tidigare krävs även hög kompetens inom data. Med IT-revolutionen har kryptering blivit en angelägenhet långt utanför det militära området.

Näringsliv och myndigheter måste ha hög kompetens vad gäller datasäkerhet. Däremot är det inte nödvändigt att man har egna

kryptologer. Ur kompetenssynpunkt räcker det dock inte med några få personer med hög kompetens inom kryptologi. För att stimulera tillväxten av särskild kompetens för samhället och de större företagen kan man exempelvis sponsra eller finansiera doktorandtjänster vid universiteten.

Beställarkompetens och revision

Samhället har, enligt utredningens mening, låg beställarkompetens för informationssäkerhet, vilket utgör ett grundläggande problem. Staten har ett ansvar för att utveckla beställarkompetensen. Tillgång till certifierade produkter enligt *Common Criteria* eller för tjänster enligt Ledningssystem för informationssäkerhet skulle avsevärt underlätta upphandling av informationssäkerhet. Det krävs också en satsning på fortbildning i upphandlingsteknik inom området informationssäkerhet, som en del i en integrerad kravspecifikation vid upphandling. Särskild uppmärksamhet bör ägnas kompetensen i avtalsfrågor.

Revision av informationssäkerhet bör utvecklas i flera former, dels som en del av den årliga revisionen, särskilt vad avser redovisnings- och affärssystem, dels genom sårbarhets- och riskanalyser och tester av informationssäkerheten samt genom tillämpning av standarden Ledningssystem för informationssäkerhet, LIS.

Informationssäkerhet är alltid en ledningsfråga. Behovet av fortbildning gäller även den verkställande nivån och styrelsenivån i myndigheter och företag. Varje myndighet, företag, kommun, landsting eller annan organisation har ett eget ansvar för att tillse att adekvat fortbildning genomförs för alla medarbetare, som har uppgifter inom området informationssäkerhet.

Signalspaningskunskap som skydd för IT-system

Signalspaningen har betydelse för möjligheten att skydda samhällsviktiga system mot kvalificerade IT-relaterade hot. Utredningen vill peka på att det finns kvalificerade IT-relaterade hot som med den framväxande globala kommunikationsstrukturen och den nya IT-tekniken i en förlängning också skulle innebära ett hot mot rikets säkerhet. Dessa hot utgör självfallet också ett hot mot många

andra verksamhetsområden. Var gränsen går mellan allmänna hot och hot mot rikets säkerhet är inte absolut.

Ett av de främsta medlen, förutom det förebyggande arbetet, för att möta de kvalificerade IT-relaterade hoten är att fokusera vår underrättelsetjänst emot dem. Detta understryks också i regeringens hittillsvarande strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas och delgivningen av erfarenheter underlättas. Signalspaningens möjligheter att spela en avgörande roll för skyddet mot kvalificerade IT-relaterade hot bedöms som stora.

När det gäller kryptologisk kompetens och förmåga har Sverige under lång tid haft en framträdande plats i Europa. Den relativt sett successivt försvagade beräkningskraften genom brist på resurser för inköp av ny snabb datorkraft riskerar dock att påverka Sveriges samlade kompetens på området.

Signalspaningen kan först och främst ge underrättelser avseende hot och aktörer som agerar mot svenska informationssystem. En lika viktig del är att kunskap om brister i olika tekniska informationssystem erhålls i den egna underrättelseverksamheten genom signalspaning. Denna kunskap bör kunna användas till skydd för samhällsviktiga system.

9 Förslag till nationell strategi

Utredningen har i kap 3 och 4 pekat på behov, möjligheter och problem inom informationssäkerhetsområdet och konstaterar att bilden av dagens brister och hot är mycket komplex och därmed även behovsbilden. För att möta denna komplexa behovsbild behövs enligt utredningen en sammanhållen politik inom informationssäkerhetsområdet, baserad på en strategi som kan omfattas av alla aktörer, privata som offentliga.

Det är nödvändigt att etablera vissa principer som kan ligga till grund för beslut om ansvarsfördelning och åtgärder i samhället. Den första principen handlar om hotets ursprung och den andra principen om hotets möjliga konsekvenser.

Enligt utredningens mening innebär den första principen att ansvaret för hanteringen av de flesta fall av administrativa och tekniska brister måste inrymmas i respektive verksamhetsansvarigs eget åtagande, vilket också följer av ansvarsprincipen. Därmed inte sagt att det offentliga åtagandet skulle utesluta hantering av konsekvenserna av dylika brister. Vissa förebyggande åtgärder, som avser det privata området, omfattas också. Helt klart är dock att det kan vara svårt för enskilda och företag att skydda sig mot aktörsberoende, antagonistiska hot. Dessa kan mycket snabbt komma att involvera staten, som måste utveckla en förmåga att hantera, och därmed förebygga, störningar, särskilt när det gäller samhällsviktig verksamhet. Var gränsen mellan det privata och det enskilda går är dock mycket svårt att slå fast.

Den andra principen innebär att ju svårare konsekvenser ett hot eller en brist kan leda till, desto mer sannolikt att staten kommer att involveras i någon form. I det statliga åtagandet bör därför ingå frågor som rör den nationella säkerheten i vid mening, till exempel krishantering, brottsbekämpning, antiterrorism eller totalförsvar.

Med dessa starkt förenklade principer för arbets- och ansvarsfördelning inom informationssäkerhetsområdet som utgångspunkt

kan fyra uppgifter eller handlingslinjer urskiljas, uppgifter som flertalet aktörer måste axla i en eller annan form, nämligen uppgiften att förebygga, förbereda, förhindra respektive att hantera allvarliga störningar. Två av dessa mål eller uppgifter – förhindra och hantera – ingår redan i regeringens strategi (prop. 2001/02:158).

Utredningen kan inte lösa problemet med informationssäkerhet helt enkelt för att det inte finns någon slutlig lösning. Därtill är problemet alldeles för brett och dessutom under ständig förändring. Utredningen ser dock att en gemensam, nationell strategi och en samverkansprocess skulle kunna lära oss att leva med problem som rör informationssäkerhet. En av utredningens huvuduppgifter är därför att se utvecklingsmöjligheter i den av regeringen angivna strategin för informationssäkerhet.

Regeringen har lagt fast den övergripande målsättningen att upprätthålla en hög informationssäkerhet i hela samhället, som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att nå detta mål, liksom för övrig krishantering i samhället, måste utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. Utredningen instämmer i regeringens bedömning och har därför inte funnit skäl att föreslå ändring i dessa grundläggande förhållningssätt.

Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) i grunden är riktig. Utredningen har dock funnit anledning att konkretisera och fördjupa den övergripande strategin i flera avseenden. I regeringens strategi ingår även vissa organisatoriska åtgärder. Utredningen har tagit fram underlag för utvärdering och återkommer till dessa frågor i slutbetänkandet.

Utredningen framhåller att en strategi för informationssäkerhet måste kunna inrymma många aspekter, tidsperspektiv, mål och medel eftersom den syftar till att sammanfatta en handlingslinje på lång sikt, en strategi som ska kunna ligga till grund både för privata och offentliga aktörer. En ökad informationssäkerhet måste därför bygga på att regeringen i en nationell strategi lyckas fånga in frågeställningar som kan omfattas av flertalet aktörer och intressenter.

Mot bakgrund av de resonemang som redovisas i kapitel 3 och 4 föreslår utredningen en strategi som innefattar att:

1. utveckla Sveriges position inom EU och i internationella sammanhang,
2. skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet,
3. främja ökad användning av IT,
4. förebygga och kunna hantera störningar i informations- och kommunikationssystem,
5. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen,
6. förstärka förmågan inom området nationell säkerhet.

I strategin bör även ingå att:

7. utnyttja samhällets samlade kapacitet,
8. fokusera på samhällsviktig verksamhet,
9. öka medvetenheten om säkerhetsrisker och möjligheter till skydd,
10. säkerställa kompetensförsörjningen.

Utredningen har valt att inledningsvis betona att de europeiska och de internationella sammanhangen är av strategisk betydelse. Informationssäkerhet är ett gemensamt, internationellt problem och de strategiska lösningarna måste därför utvecklas i samverkan med andra länder, både inom EU och i internationella organ. En bred tillämpning av OECD:s riktlinjer är därvid ett viktigt steg. Förmågan att samordna arbetet behöver utvecklas, dels för att fullfölja svenska positioner och åtaganden, men också för att bättre ta tillvara de erfarenheter som alla andra internationella aktörer gör.

Den andra och tredje punkten är nationell till sin karaktär i den meningen att ansvar, befogenheter och resurser redan finns att förfoga över. Utredningen vill betona att den ökade informationssäkerheten skall stödja en svensk utveckling av näringsliv och offentlig sektor och skall främja en demokratisk utveckling och ökad trygghet för medborgarna. Detta innebär att förtroendet för informationsförsörjning måste kunna upprätthållas, även när den sker elektroniskt. En väl fungerande informationsförsörjning bygger på att informationssäkerheten kan utvecklas, vilket i sin tur är en förutsättning för ökad användning av IT. Detta är också en förutsättning för tillväxt, konkurrens och utveckling.

I regeringens övergripande strategi ingår formuleringen att ”kunna förhindra och hantera störningar i samhällsviktig verk-

samhet". Utredningen menar att i strategin bör tydliggöras vikten av *förebyggande* och förberedande åtgärder, eftersom detta stärker förmågan att förhindra och effektivt kunna hantera störningar och konsekvenserna som kan följa därav. Vidare betonar utredningen att begreppet hantera måste inkludera förmågan att i olika former ingripa och agera i samband med störningar, till exempel genom brottsbekämpning. Till säkerhetsbegreppet hör att utvärdera och återföra erfarenheter för en ökad robusthet och säkerhet i framtida verksamhet. Dessa kompletteringar skall klargöra att informationssäkerhetsarbete måste omfatta alla skeden och flera aktörer. Det innebär att den förebyggande uppgiften och de förberedande åtgärderna måste bli en del av många myndigheters sektorsansvar och instruktionsmässiga uppgift. Utredningen föreslår vidare att regeringens strategi i denna fråga preciseras till att avse störningar i informations- och kommunikationssystem. Frågan om prioriteringar av samhällsviktig verksamhet föreslås behandlas som en särkilt punkt i strategin.

Regeringen har tidigare konstaterat att för att förhindra allvarliga informationsattacker mot svenska intressen bör underrättelse- och säkerhetstjänsternas arbete förstärkas. Utredningen delar denna uppfattning men framhåller samtidigt att flera aktörer måste kunna få del av underrättelseinformationen för att kunna beakta denna i sin eget säkerhetsarbete. Utredningen är väl medveten om de restriktioner och svårigheter som ligger i uppgiften men framhåller ändå att bearbetning inriktning och delgivning av underrättelseinformation måste utvecklas i syfte att ge underlag för alla aktörer med uppgifter inom informationssäkerhetsområdet.

En av de grundläggande principerna för ansvars- och arbetsfördelningen på informationssäkerhetsområdet innebär att ju svårare konsekvenser ett hot eller en brist kan leda till, desto mer sannolikt att staten kommer att involveras i någon form. I det statliga åtagandet bör därför ingå frågor som rör den nationella säkerheten i vid mening, till exempel krishantering, brottsbekämpning inklusive kontraterrorism eller totalförsvar. För att möta de mest kvalificerade hoten krävs, enligt utredningens mening, en förstärkt förmåga att upptäcka och analysera störningar liksom en förmåga att kunna ingripa och agera kraftfullt mot antagonistiska aktörer. Utan en helhetssyn på de tekniskt relaterade hoten kommer staten inte att kunna skydda samhället från kvalificerade aktörers angrepp på svenska informationssystem. En sådan helhetssyn förutsätter tillgång till relevant information, kompetens och

teknisk utrustning, frågor som kräver långsiktighet och uthållighet och därför bör innefattas i en nationell strategi.

I dessa första sex punkter har utredningen försökt sammanföra frågeställningar och överväganden som handlar om strategiska målsättningar. Utredningen har även funnit anledning att föreslå inriktning och prioriteringar av det kommande informationssäkerhetsarbetet i syfte att stödja regeringens övergripande mål att upprätthålla hög informationssäkerhet i samhället. Dessa förslag bör också ingå i en långsiktig strategi.

Mot denna bakgrund föreslår utredningen att utgångspunkten för informationssäkerhetsarbetet bör vara att bättre utnyttja samhällets samlade kapacitet på området. De investeringar som redan gjorts i människor, kompetens och teknik utgör en värdefull potential för framtiden. Ökad informationssäkerhet handlar därför enligt utredningens synsätt inte i första hand om ytterligare investeringar utan snarare om en tydligare ansvars- och arbetsfördelning mellan samhällets olika aktörer. Den tekniska utvecklingen på IT-området är i allt väsentligt styrd av olika privata aktörer på marknaden. Eftersom utvecklingen finns i marknaden är det också där som säkerhetslösningar måste utvecklas. Inom samhällsviktiga områden måste därför aktörerna inom offentlig sektor utveckla sina förutsättningar och sin förmåga som kravställare och beställare. Enligt utredningens mening borde det vara möjligt att inom ytterligare sektorer utveckla samverkan i syfte att öka informationssäkerheten, särskilt om uppgiften att förebygga och förbereda tydliggörs för ytterligare myndigheter med sektorsansvar som involverar näringslivet som aktörer. Utredningen har vid flera tillfällen kunnat konstatera att olika representanter för näringslivet välkomnar en bredare samverkan kring informationssäkerhet till ömsesidig nytta men att denna samverkan måste vila på frivillighet. Att utveckla former för samverkan mellan det privata och offentliga är mot denna bakgrund av strategisk betydelse.

Utredningen menar, liksom regeringen, att det av flera skäl är nödvändigt att fokusera ansträngningarna till sådana verksamheter som är av vital betydelse för samhällets funktioner. En verksamhet måste således betraktas som samhällsviktig om ett bortfall eller en störning av denna skulle få allvarliga konsekvenser för en eller flera samhällsfunktioner. Det är uppenbart att leveranssäkerheten och kvaliteten i den tekniska infrastrukturen kommer att vara beroende av hur informationssäkerheten i dessa system utvecklas. Men även många andra samhällstjänster är beroende av säkerheten i informa-

tions- och kommunikationssystemen. En helhetssyn på informationssäkerheten i samhällsviktiga verksamheter blir därför allt viktigare. Eftersom samhällets resurser inte är obegränsade kommer därför en prioritering mellan samhällsviktiga verksamheter också att vara av strategisk betydelse.

IT-området utvecklas snabbare än säkerhetsmedvetandet. Det ökade IT-användandet har lett till ett ökat beroende av säkerhet och kvalitet i olika tjänster men medvetandet om sårbarheter, hot och risker är i dagsläget mycket lågt hos enskilda användare. Detsamma gäller kunskapen om vilka skyddsåtgärder som finns och erbjuds på marknaden. Enligt utredningens mening är medvetandet i dag så dåligt och bristerna så utbredda att särskilda insatser är motiverade under lång tid.

En rad åtgärder måste, enligt utredningen vidtas för att ytterligare förbättra säkerhetsmedvetandet och öka kunskaperna. Det bör bland annat ske inom ramen för utbildningssystemet. Lärarutbildningen måste förbättras och säkerhetsmedvetande, anpassat till respektive ålders behov och förutsättningar, måste byggas in i skolans grundläggande data- och IT-utbildning i såväl grund- som gymnasieskolan. En betydande del av utbildningsbehovet måste tillgodoses inom högskolans ram. Kopplingen måste stärkas mellan utbildning och forskning. Informationssäkerhet bör utgöra en baskunskap för många yrkesgrupper, alltifrån jurister, samhällsvetare, lärare och ekonomer till tekniker. Det finns skäl att stimulera till etablering av kvalificerad utbildning i informationssäkerhet på magisternivå för att bland annat tillgodose efterfrågan av tjänster inom området. De växande behoven av säkra informationssystem ställer också krav på ökade resurser för forskning inom informationssäkerhet. Enligt utredningens mening är det således av strategisk betydelse att kunna säkerställa kompetensförsörjningen inom informationssäkerhetsområdet.

I dessa tio punkter har utredningen sammanfattat sin syn på vad som bör ingå i en nationell informationssäkerhetsstrategi. Strategin har ett långsiktigt perspektiv och skall kunna ligga till grund för handlingsplaner, prioriteringar och åtgärder på två till tre års sikt, vilka kan förnyas utifrån ändrade omständigheter. Strategin vänder sig till alla aktörer, såväl privata som offentliga. Strategin kan ligga till grund för att öka informationssäkerheten i samhället genom en kontinuerlig process.

10 Handlingsprogram; förslag till åtgärder

Med utgångspunkt i förslaget till nationell strategi redovisar utredningen ett förslag till handlingsprogram med förslag till åtgärder. Staten förfogar i princip över en rad administrativa, ekonomiska och informativa styrmedel. I praktiken är dessa svagt utvecklade inom området informationssäkerhet. Utredningen lämnar därför bland annat förslag till fortsatt författningsarbete och tillämpning av standard för att uppnå en godtagbar nivå.

Utredningen föreslår även en målstruktur för informationssäkerhet som kan medverka till en mera sammanhållen politik för informationssäkerhet. Utredningen har inte sett som sin uppgift att skapa en ny terminologi för informationssäkerhet utan använder det språkbruk som anges i SIS terminologi för informationssäkerhet och de begrepp som EU använder[1]. Det man vill uppnå är konfidentialitet, okränkbarhet och tillgänglighet.

Informationssäkerhet är en angelägenhet för hela samhället. Behovet är inte begränsat till verksamheter av betydelse för rikets säkerhet eller skyddet mot terrorism. Behovet är inte heller begränsat till information som är hemlig enligt sekretesslagen. Informationssäkerhet är inte en åtgärd vid extraordinära händelser, utan ett vardagskrav för god funktion.

Olika aktörer, som offentlig sektor, privat sektor och medborgare, har olika behov av informationssäkerhet, men också skiftande ansvar och skyldigheter. Alla aktörer har inte samma möjligheter att bidra till informationssäkerhet utanför den egna verksamheten.

[1] Informationssäkerhet definieras av SIS som säkerhet rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spårbarhet och oavvislighet. EU definierar informationssäkerhet som ”förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten (autentisering), integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät”.

Begrepp

- Ansvarsprincipen, närhetsprincipen och likhetsprincipen så som de definieras i krishanteringssystemet bör tillämpas även för informationssäkerhet.
- Ett begrepp som visat sig grundläggande i utredningens arbete är samhällsviktig verksamhet. Utredningen anser att det finns ett starkt behov av att definiera vilka kriterier som skall uppfyllas för att en verksamhet eller ett system skall betraktas som samhällsviktig.

Nationellt ansvar och internationella åtaganden

- Inhemska huvudaktörer på informationssäkerhetsområdet är stat, kommuner och landsting samt näringslivet. De har eget ansvar för sina respektive områden, men också möjligheter att tillsammans utveckla informationssäkerheten i hela samhället. Staten skall ta huvudansvar för att utveckla samverkansformer.
- Uppgiften att förebygga allvarliga incidenter bör bli en del av många myndigheters sektorsansvar och instruktionsmässiga uppgift.
- Staten bör träffa ett avtal med Sveriges Kommuner och Landsting inom området informationssäkerhet.
- Etermedias beroende av funktionalitet och fungerande system för informationssäkerhet bör uppmärksammas såväl i produktion som i distribution.
- Staten har ansvar för skyddet mot IT-attacker från främmande land eller från andra allvarliga antagonistiska aktörer som drabbar Sverige. Utredningen anser att staten måste ha en kvalificerad teknisk kompetens för att kunna förebygga och förhindra nationella kriser med IT-inslag, liksom för att kunna testa säkerheten i verksamheter av stor betydelse för rikets säkerhet eller för samhällets funktionsförmåga.
- Förmågan att kunna respondera vid incidenter i informationssäkerhet måste utvecklas i ett nära internationellt samarbete.
- Möjligheterna till helhetssyn måste förbättras. Helhetssyn kräver tillgång till relevant information, såväl öppen som

hemlig. Det förutsätter deltagande även från underrättelse- och säkerhetstjänsterna.

- Sveriges agerande i det internationella samarbetet kring informationssäkerhet måste samordnas, liksom svenska ställningstaganden i policyfrågor.
- Sverige måste också säkerställa en hög teknisk kompetens för att kunna vara en aktiv aktör och en attraktiv partner i EU och i internationellt samarbete.
- Det arbete som genomförs inom EU måste syfta till att öka nät- och informationssäkerheten och därigenom stärka integriteten och tillgängligheten.

Utredningens förslag innebär en implementering av OECD:s riktlinjer till svenska förhållanden.

Säkrare Internet

- Infrastrukturen för Internet som består av såväl fysiska som logiska element måste skyddas för att möjliggöra ett säkrare Internet. Operatörerna bör både ha möjlighet och skyldighet att vidta förebyggande åtgärder. Hit hör också att skydda mot avbrott och störningar i elförsörjningen.

Författningsfrågor

- Författningsändringar är nödvändiga. Det behövs ett utvidgat, mera sammanhållet och heltäckande regelverk som motsvarar utredningens bredare definition av begreppet informationssäkerhet. Utredningen förordar en helt ny lag på informationssäkerhetsområdet. Framtagandet av ett sådant regelverk måste dock föregås av en omfattande och djupgående analys, vilket kräver en särskild utredning.
- Utredningen föreslår ändå lagstiftningsåtgärder för att råda bot på vissa brister i dagens regelverk. En ny förordning föreslås om vissa åtgärder för informationssäkerhet hos staten.

- Begreppet informationssäkerhet föreslås utmönstras ur säkerhetsskyddslagstiftningen för att ersättas med begreppet sekretessäkerhet.

Standarder

- Att få fram en bra basnivå för alla myndigheters informationssäkerhet underlättar möjligheterna att revidera säkerheten, liksom för Säkerhetspolisens författningsreglerade arbete med rådgivning och kontroll.
- För att förbättra informationssäkerheten föreslår utredningen att staten skall gå i bräschen för en bred användning av standarder för informationssäkerhet inom i princip all statlig verksamhet.
- EU har pekat ut standarderna *Common Criteria* och Ledningssystem för informationssäkerhet, LIS, som grunder för informationssäkerhet. Statskontorets startpaket OffLIS bör tills vidare utgöra ett rekommenderat stöd vid införandet av LIS i statlig verksamhet.
- Datainspektionens allmänna råd bör relateras och närmas till LIS. En översyn är aviserad med detta syfte under 2005.

Målstruktur; finansiell styrning

- I statens målstruktur bör informationssäkerhet vara ett verksamhetsområde. Ett exempel på ett målresonemang skulle kunna vara kravet på robusthet och säkerhet inom samhällsviktiga verksamheter och övergripande mål som avser krav på prestationsförmåga eller tillgänglighet. Övergripande krav bör formuleras i måltermer, inte som krav på vissa tekniska lösningar.
- På nivån verksamhetsgren kan säkerhetsmål vara generella krav på tillämpning av standarder eller krav på lägsta godtagbara funktionsförmåga, dels normalt, dels under störda förhållanden. Vid koncessioner bör säkerhetskrav arbetas in i koncessionsvillkoren.

- På myndighetsnivå kan målen för informationssäkerhet formuleras som operativa prestationsmål, krav på tillgänglighet, specifik tillämpning av standarder, krav på säkerhetspolicy, samt krav på tester och revision av säkerheten.
- Med utgångspunkt i ansvarsprincipen är det rimligt att finansiering av informationssäkerhet i huvudsak sker genom ordinarie anslag. Att ta ut avgifter som i praktiken används för att finansiera informationssäkerhet för de som erlagt avgifterna kan vara möjligt inom till exempel teknisk infrastruktur.
- Det är enligt utredningen motiverat att även i framtiden – särskilt för ändamål som kan ses som långsiktiga investeringar i en högre informationssäkerhet – behålla möjligheterna till kompletterande finansiering via den s.k. civila ramen.

Säkerhetsmedvetande

- Det finns starka skäl att öka insatserna för ett brett säkerhetsmedvetande. Främst gäller det att öka medvetenheten om sårbarhet och risker, men också om metoder och åtgärder för en säkrare IT-användning.
- Information kan vara ett hushålls, företags eller ett samhälles allra viktigaste tillgångar som måste kunna skyddas. Som enskilda individer måste vi alla vara beredda ta personligt ansvar för informationssäkerhet upp till en viss nivå.
- Säkerhetsmedvetande, anpassat till respektive ålders behov och förutsättningar, måste byggas in i skolans grundläggande data- och IT-utbildning i såväl grund- som gymnasieskolan.

Utbildningsfrågor

- I grund- och gymnasieskolan måste kunskap om informationssäkerhet komma in tidigt i undervisningen. I dagens gymnasium har eleverna redan använt datorer och Internet i många år. Kunskap om informationssäkerhet tas i gymnasiet främst upp från ett tekniskt perspektiv. Det leder lätt till uppfattningen att säkerhet är något som tekniker skall leverera utan att andra behöver tänka på problemet.

- Lärarutbildningarna måste utvecklas så att kunskap om och förståelse för IT-utvecklingen i samhället blir obligatorisk. Det bör särskilt ske med fokus på de möjligheter och problem som finns kring IT i skolan, både som läromedel men även som administrativt hjälpmedel och som säkert redskap för kommunikation.
- En betydande del av utbildningsbehovet kring informationssäkerhet måste tillgodoses inom högskolans ram. Kopplingen måste stärkas mellan utbildning och forskning.
- Informationssäkerhet bör utgöra en baskunskap för många yrkesgrupper, alltifrån jurister, samhällsvetare, lärare och ekonomer till tekniker. Utredningen förordar att frivilliga men rekommenderade kurser i informationssäkerhet på 3–5 poäng införs i bland annat utbildningarna till civilingenjör, civilekonom, jurist och samhällsvetare, samt motsvarande i efterutbildningen av läkare. För systemvetare och dataingenjörer bör en sådan kurs vara obligatorisk med möjlighet till ytterligare fördjupning.
- Det finns skäl att stimulera till etablering av kvalificerade utbildningar för blivande chefer i informationssäkerhet. Det finns behov av sådan utbildning på magisternivå (mastersnivå) efter akademisk examen.
- Det finns behov av att förstärka kompetensen inom IT-relaterad kriminalteknisk (IT-forensisk) verksamhet.

Forskning

- För att utveckla kunskap och kompetens inom ett delvis nytt ämnesområde som informationssäkerhet behöver forskning initieras, stimuleras och följas upp. Det är viktigt att utifrån god överblick och bedömningsförmåga inrikta forskningen mot nydanande mångvetenskapliga perspektiv. Forskningsbaserad kunskap bygger på långsiktighet och uthållighet i projektsatsningar och i kompetensutveckling bland berörda forskare.
- Krisberedskapsmyndigheten bör utveckla ett tematiskt forskningsområde kring informationssäkerhet. Forskargrupper som erhåller stöd bör veta att satsningen är flerårig. Det är en kvalitativ aspekt som också är väsentlig för att inom landet

skapa kompetens och personliga förmågor att samverka internationellt inom ämnesområdet.

- Utbildning i informationssäkerhet bör också ske vid Försvarshögskolan med en praktisk inriktning för certifiering av nyckelpersonal inom myndigheter och företag, samt med en teoretisk magisterutbildning för fördjupade kunskaper inom ämnesområdet.
- Utredningen betonar vikten av samarbete mellan offentlig och privat sektor. Sics, the Swedish Institute for Computer Science, fyller tillsammans med övriga samverkande institut, en mycket viktig funktion för att vara en avancerad brygga mellan näringslivets forskningsbehov, statens behov att främja forskningen och forskarvärlden inom IT-området. Utredningen anser att institutens forskning bör få en tydligare inriktning även på forskning inom området informationssäkerhet.

Internationell forskarsamverkan

- Sverige bör ha en hög ambition att delta såväl i EU:s policyskapande arbete för att inrikta forskningen inom informationssäkerhetsområdet och som avnämare och genomförare av större forskningsprojekt inom området. Det är en angelägen uppgift för bland annat Regeringskansliet, Krisberedskapsmyndigheten och Vinnova, liksom för svenskt näringsliv och universitets- och högskolevärlden att delta i arbetet och få del av de betydande forskningsresurser EU satsar på området.
- Till Sveriges ambitioner på forskningsområdet måste höra att utveckla samarbete med partners i andra länder eftersom EU-finansierade forskningsprojekt ofta förutsätter samverkan mellan aktörer i flera medlemsländer.

Kryptokompetens

- Näringsliv och myndigheter måste ha en hög kompetens på kryptoområdet. För att stimulera tillväxten av särskild kompetens bör man överväga att sponsra eller finansiera doktorandtjänster inom kryptologi. Det är också en fördel att kunna

använda inhemska leverantörer av utrustning som kan tillhandahålla källkod för utvärdering.

Beställarkompetens

- Beställarkompetensen inom området informationssäkerhet behöver stärkas. Det kan bland annat ske genom att successivt infoga kravet på certifiering vid upphandling eller outsourcing, men även genom att tillämpa kvalitetskraven i Ledningssystem för informationssäkerhet, LIS.
- Utredningen föreslår också en satsning på fortbildning i upphandlingsteknik inom området informationssäkerhet, som en del i en integrerad kravspecifikation vid upphandling.
- Ökade krav från statens sida vid upphandling kan också förväntas öka förutsättningarna för svensk IT-industri att kunna leverera säkra produkter och system och därvid även stärka sin konkurrensförmåga på den internationella marknaden.
- Företeelsen outsourcing, det vill säga lägga ut viktiga delar av verksamheten till exempel inom IT-området på entreprenad, ökar kraftigt kravet på långsiktig beställarkompetens. Frågeställningen har stor giltighet även för kommuner och landsting.
- Revision av informationssäkerhet måste utvecklas. Utredningen anser det angeläget att Riksrevisionens projekt om förbättrad säkerhetsrevision behandlas skyndsamt.

Underrättelse- och säkerhetstjänst

- Underrättelse- och säkerhetstjänsterna behöver förstärkas.
- I det statliga åtagandet bör därför ingå frågor som rör den nationella säkerheten i vid mening, till exempel krishantering, brottsbekämpning inklusive kontraterrorism eller totalförsvar. För att möta de mest kvalificerade hoten krävs, enligt utredningens mening, en förstärkt förmåga att upptäcka och analysera störningar liksom en förmåga att kunna ingripa och agera kraftfullt mot antagonistiska aktörer.
- Bättre rutiner bör skapas för att ta tillvara den information som finns i underrättelseorganen. Metoder för inriktning, bearbet-

ning och delgivning bör utvecklas för att ge underlag för en bättre helhetsbild av de risker och hot som finns inom informationssäkerheten.

Signalspaning

- På liknande sätt som Sverige kunnat ta tillvara signalspaningens unika kompetens för att skydda kryptosystem, bör man även kunna ta tillvara den kunskap om brister i IT-säkerhet som utvecklats inom signalspaningen. Det har betydelse för möjligheten att skydda samhällsviktiga system mot kvalificerade IT-relaterade hot.
- Signalspaning har en central roll såväl för offensiv förmåga (underrättelseinhämtning) som för defensiv förmåga (signalskydd och IT-säkerhet), vilket inte alltid framgår av den offentliga debatten då verksamheten omgärdas av hög sekretess. Den offensiva aspekten är avgörande även för den defensiva förmågan, på samma sätt som kryptoskyddet är avgörande för det traditionella signalskyddet.

Organisationsfrågor

- Utredningen återkommer i slutbetänkandet till frågor med organisationspåverkan.

11 Författningsförslag Specialmotiveringar

11.1 Förslaget till förordning (0000:000) om vissa åtgärder för informationssäkerhet hos staten

Inledande bestämmelser

> 1 § I denna förordning ges bestämmelser om vissa åtgärder för att säkerställa administrativ och teknisk informationssäkerhet hos statliga myndigheter under regeringen.
>
> Bestämmelserna i denna förordning skall tillämpas bara om något annat inte följer av lag eller annan förordning.

Av paragrafen följer att bestämmelserna i förordningen inte avser själva informationen som behandlas utan de åtgärder som skall vidtas för att säkerställa säkerheten för denna. Bestämmelserna avser således säkerheten vid hanteringen av elektroniska system för bearbetning, lagring och överföring av information.

I säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633), personuppgiftslagen (1998:204) m.m. finns regler om informationssäkerhet som alltid skall gälla oavsett vad som i denna förordning föreskrivs om administrativa och tekniska åtgärder.

> 2 § Med administrativ och teknisk informationssäkerhet avses i denna förordning säkerhet vid hantering av elektroniska system för bearbetning, lagring och överföring av information, för att i den elektroniska hanteringen säkerställa informationens konfidentialitet, okränkbarhet och tillgänglighet.

I paragrafen definieras vad som i förordningen avses med administrativ och teknisk säkerhet.

Av definitionen följer att förordningen reglerar IT-säkerhet och inte informationssäkerhet i hela dess vidd.

> 3 § En myndighet skall säkerställa den administrativa och tekniska informationssäkerheten genom att vidta de administrativa och tekniska åtgärder som anges i 4–8 §§.
>
> Regeringen kan besluta att de myndigheter som anges i bilagan till denna förordning skall tillämpa särskilda säkerhetskrav utöver de grundkrav som anges i denna förordning.

De myndigheter för vilka särskilda säkerhetskrav kan gälla finns upptagna i bilaga till förordningen.

Administrativa åtgärder

Informationssäkerhetsplan

> 4 § Myndigheten skall upprätta riktlinjer för informationssäkerheten och en årlig plan för administrativa och tekniska åtgärder inom myndigheten för att säkerställa att ställda krav på informationssäkerhet uppnås.
>
> Planen skall utformas med hänsyn till övriga krav som ställs i verksamheten. Planen skall innehålla en redovisning av de systemspecifika säkerhetskrav som utarbetas av myndigheten för driften av IT-system. Redovisningen av systemspecifika säkerhetskrav skall vara fullständig och tydlig samt ange de säkerhetsprinciper som skall följas och vilka detaljerade säkerhetskrav som skall uppfyllas. Planen skall även innehålla en översikt över de åtgärder som genomförts enligt 5–8 §§.

Med riktlinjer för informationssäkerheten avses en informationssäkerhetspolicy som beslutas av myndighetschefen. Informationssäkerhetsplanen tar sikte på det operativa arbetet.

Informationssäkerhetsansvarig

> 5 § Hos myndigheten skall det finnas en informationssäkerhetsansvarig som utövar kontroll över informationssäkerheten. Den informationssäkerhetsansvarige skall i dessa frågor vara direkt underställd myndighetens chef. Det skall finnas ersättare för den informationssäkerhetsansvarige.

Myndighetens chef är huvudansvarig för informationssäkerheten vid myndigheten. Den informationssäkerhetsansvarige skall därför

i informationssäkerhetsfrågor vara direkt underställd myndighetens chef. Paragrafen reglerar dock inte den informationssäkerhetsansvariges organisatoriska hemvist. Av stadgandet framgår också att det skall finnas en eller flera ersättare för den informationssäkerhetsansvarige.

Behörighet

6 § Tillgång till viss utrustning eller information som är specifik för systemens säkerhet skall kräva särskild behörighet.

I paragrafen anges att det i vissa fall skall krävas särskild behörighet för tillgången till viss utrustning eller information. De närmare kriterierna får utformas i föreskrifter.

Utbildning

7 § Myndigheter skall se till att personal med arbetsuppgifter där hantering av elektroniska system för bearbetning, lagring och överföring av information ingår får utbildning om informationssäkerhet.

Tekniska åtgärder

8 § Myndigheten svarar för att tekniska åtgärder vidtas så att sådan utrustning m.m. som används för, eller stödjer användandet av, system vid elektronisk bearbetning, lagring och överföring av information uppfyller grundläggande krav på informationssäkerhet. Myndigheten svarar även för att kraven på informationssäkerheten kan upprätthållas då utomstående anlitas för tjänster som rör myndighetens informations- och kommunikationssystem. För vissa myndigheter (i bilaga) kan därutöver gälla särskilda krav på tekniska åtgärder.

I paragrafen anges att en myndighet även svarar för att kraven på informationssäkerheten kan upprätthållas även vid anlitandet av utomstående till exempel olika operatörer.

Tillsyn

9 § Informationssäkerheten enligt denna förordning skall kontrolleras av den myndighet som regeringen bestämmer.

10 § Om det vid tillsynen över informationssäkerheten enligt denna förordning framkommer brister som trots påpekande inte rättas till, skall tillsynsmyndigheten anmäla förhållandet till regeringen.

Bestämmelsen innebär att brister i den informationssäkerhet som förordningen avser skall komma till regeringens kännedom.

Verkställighetsföreskrifter

11 § Den myndighet som regeringen bestämmer skall meddela närmare föreskrifter om de administrativa och tekniska åtgärder som skall vidtas för att uppfylla grundläggande och särskilda krav på informationssäkerhet vid hantering av elektroniska system för bearbetning, lagring och överföring av information.

11.2 Förslaget till lag om ändring i säkerhetsskyddslagen (1996:627)

7 § Säkerhetsskyddet skall förebygga
1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (*sekretess-säkerhet*),
2. att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning), och
3. att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Säkerhetsskyddet skall även i övrigt förebygga terrorism.

Sekretessäkerhet

9 § Vid utformningen av *sekretessäkerheten* skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt.

Ändringarna innebär att begreppet informationssäkerhet i säkerhetsskyddslagen (1996:627) ersätts med begreppet sekretessäkerhet. Ändringarna föranleds av vad som i avsnitt 7.3 sägs om behovet av en utmönstring av begreppet informationssäkerhet ur säkerhetsskyddslagstiftningen.

11.3 Förslaget till förordning om ändring i säkerhetsskyddsförordningen (1996:633)

Sekretessäkerhet

9 § Hemliga handlingar som är av synnerlig betydelse för rikets säkerhet skall inventeras minst en gång per år. Andra hemliga handlingar skall inventeras i den omfattning som anges i föreskrifter enligt 45 §.

13 § Myndigheter och andra som förordningen gäller för skall, innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, förvissa sig om att det för uppgifterna där finns fullgod *sekretessäkerhet*.

Ändringen innebär att begreppet informationssäkerhet i säkerhetsskyddsförordningen (1996:633) ersätts med begreppet sekretessäkerhet. Ändringen föranleds av vad som i avsnitt 7.3 sägs om behovet av en utmönstring av begreppet informationssäkerhet ur säkerhetsskyddslagstiftningen.

Akronymlista

AQUA	Appropriately Qualified Authority
BITS	Basnivå för IT-säkerhet
CATS	Centrum för Asymmetriska hot och Terrorism-studier
CCRA	Common Criteria Recognition Arrangement
CEN	The European Committee for Standardization
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
DCS	Dependable Computer Systems
DNS	Domännamnssystemet
DNSSEC	DNS Security Extensions
DS	Departementsserien
eECC	e-Europa Smart Card
EG	Europeiska Gemenskapen
EkomL	Lagen om elektronisk kommunikation
Enisa	Europeiska nät- och informationssäkerhetsbyrån
ESFP	Den gemensamma utrikes och säkerhetspolitiken

EU	Europeiska Unionen
FDA	Food and Drug Administration
FHS	Försvarshögskolan
FMV	Försvarets materielverk
FOI	Totalförsvarets Forskningsinstitut
FRA	Försvarets radioanstalt
GMITS	Guidelines for the Management of IT security
GOV NET	Government Network
GSM	Global System for Mobile Communications
GUSP	Den gemensamma utrikes- och säkerhetspolitiken
HTML	Hyper Text Markup Language
IDS	Image Display System
IEC	International Electrotechnical Commission
IHT	Institutet för högre totalförsvarsutbildning
IKT	Informations- och kommunikationsteknik
IP	Internet Protocol
IRI	Institutet för Rättsinformatik
ISO	International Organization for Standardization
IST	Informationssamhällets teknik
IT	Informationsteknik
ITiS	IT i skolan
ITS	Informationstekniska standardiseringen
ITU	Internationella Teleunionen
JSR	Joint Research Centre

KBM	Krisberedskapsmyndigheten
KK-stiftelsen	Stiftelsen för kunskaps- och kompetensutveckling
KOM	Kommissionen
KTH	Kungliga Tekniska Högskolan
LAN	Local Area Network
LIS	Ledningssystem för informationssäkerhet
LPO	Läroplan för det obligatoriska skolväsendet
MICTS	Management of Information and Communications Technology Security
MS	Microsoft
NCSA	National Communication Security Agency
OECD	Organisation on Cooperation and Development
OffLIS	LIS för offentlig förvaltning
PASR	Preparatory Action on Security Resolution
PTS	Post- och telestyrelsen
PUL	Personuppgiftslagen
RÖS	Röjande signaler
SEK	Svenska Elektriska kommissionen
Sics	The Swedish Institute of Computer Science
SIS	Standardisering i Sverige
SITI	Svenska IT-institutet
SITIC	Sveriges IT-incidentcentrum
SITCEN	Situation Centre
SOU	Statens Offentliga Utredningar

SUA	Säkerhetsavtal i upphandlingssammanhang
SWEDAC	Styrelsen för ackreditering och teknisk kontroll
TSA	Totalförsvarets signalskyddssamordning
USA	United States of America
UTC	Universal Time Coordinated
VPN	Virtual Private Network
VLAN	Virtuellt LAN

Kommittédirektiv

Angående vissa frågor om informationssäkerheten i samhället

Dir. 2002:103

Beslut vid regeringssammanträde den 11 juli 2002

Sammanfattning av uppdraget

En utredare skall lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. I uppdraget ingår att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten.

Den särskilda utredaren kommer också att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren planeras också få uppdraget att genomföra den utvärdering som regeringen aviserat i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158).

Regeringen avser att återkomma under hösten med tilläggsdirektiv när det gäller dessa uppdrag.

Inledning

I takt med att samhället har blivit allt mer beroende av olika informationssystem har vikten av att förbereda sig för hot av olika slag ökat. Regeringen har närmare beskrivit hotbilden för attacker via informationssystem i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 104 f). Där konstateras att en av svårigheterna med hanteringen av de IT-relaterade hoten är att urskilja vem aktören är, eftersom ingen absolut åtskillnad mellan olika typer av aktörer kan göras. Detta faktum gör att det är särskilt svårt att skydda sig eftersom säkerhetsåtgärderna måste anpassas till samtliga typer av aktörer. Ytterligare en försvårande faktor är att de IT-relaterade hoten är geografiskt gränslösa. Den som vill göra

intrång i eller på annat sätt manipulera ett informationssystem i Sverige kan befinna sig var som helst i världen.

Signalskyddsverksamheten

Att skydda information som utväxlas i form av meddelanden och trafik eller information som lagras elektroniskt får allt större betydelse i dagens samhälle. Det gäller inte bara för sådan information som omfattas av bestämmelserna om sekretess i sekretesslagen (1980:100), utan också för andra uppgifter som hanteras i informationssystem av olika slag i samhället. Exempel på sådan skyddsvärd information kan vara uppgifter som gäller känslig infrastruktur, ekonomi och personlig integritet.

Utvecklingen av dagens signalskyddssystem sker till största delen inom Försvarsmakten utifrån de krav som behovet av att kunna hantera information som omfattas av sekretess till skydd för rikets säkerhet ställer. Utvecklingen av IT-säkerhetslösningar i samhället i övrigt styrs allt mer av behovet av att skydda information som inte omfattas av sekretess till skydd för rikets säkerhet. En utveckling av signalskyddstjänsten till att även kunna hantera andra kryptografiska skyddsbehov än de som utvecklas för totalförsvarsändamål och en bedömning av hela samhällets skyddsförmåga är därför påkallad.

Signalskyddstjänsten leds idag av en funktion inom Försvarsmakten (MUST/TSA). Att signalskyddstjänstens ledning organisatoriskt har denna placering kan innebära en risk för att de civila behoven inte prioriteras tillräckligt. Frågan om var signalskyddstjänsten på nationell nivå skall organiseras och lokaliseras bör därför övervägas.

I propositionen Ett informationssamhälle för alla (prop. 1999/2000:86) angav regeringen att den välkomnar en bred användning av kryptografi. Mot denna bakgrund bör det eventuellt finnas en rådgivande funktion i kryptografifrågor i Sverige. Därför finns behov av att undersöka i vad mån signalskyddstjänsten kan utgöra ett sådant rådgivande organ i samhället.

Det ökade samarbetet med andra stater och internationella organisationer medför vidare ett ökat statligt behov av att kunna hantera signalskyddsutrustning och kryptonycklar även i internationella sammanhang. Det bör övervägas om signalskyddstjänsten kan bistå i den utvecklingen.

Arbetet med informationssäkerhet inom offentlig sektor

Regeringen har i propositionerna Fortsatt förnyelse av totalförsvaret (prop. 2001/02:10, bet. 2001/02:FöU02, rskr. 2001/02:91) och Samhällets säkerhet och beredskap (prop. 2001/02:158, bet. 2001/02:FöU10, rskr 2001/02:261) redovisat sin strategi och förslag till åtgärder för att stärka informationssäkerheten i samhället och skyddet av de samhällsviktiga systemen. I propositionen Samhällets säkerhet och beredskap vidgades åtgärderna från att endast omfatta IT-säkerhet till att täcka hela informationssäkerhetsområdet. Det tidigare använda mer oprecisa begreppet ”informationsoperationer” utmönstrades därmed ur terminologin.

Regeringen har angett att målet bör vara att man skall upprätthålla en så hög informationssäkerhet i hela samhället att störningar i samhällsviktig verksamhet kan förhindras eller hanteras. Strategin för att uppnå detta mål liksom för övrig krishantering i samhället utgår från ansvarsprincipen, likhetsprincipen och närhetsprincipen.

Som ett första steg i en samlad strategi i informationssäkerhetsarbetet har fyra myndigheter fr.o.m. andra halvåret 2002 fått nya uppgifter. Dessa myndigheter är Krisberedskapsmyndigheten, Post- och telestyrelsen, Försvarets radioanstalt och Försvarets materielverk.

Detta första steg skall utvärderas efter två år som regeringen förutskickat i propositionen Samhällets säkerhet och beredskap.

Med anledning av att det finns många företag som är verksamma inom informationssäkerhetsområdet finns det dock skäl att ytterligare överväga vilken verksamhet staten skall bedriva inom detta område. Härvid skall beaktas att konkurrensen på den öppna marknaden inte får påverkas negativt.

Regeringen finner att de bästa förutsättningarna för ett gott beslutsunderlag kan skapas genom att utvecklingen inom informationssäkerhetsområdet följs.

Internationell verksamhet

Genom att hoten mot informationssystemen inte bara är en svensk angelägenhet, utan är av global natur, krävs internationell samverkan. Sådan samverkan bedrivs på flera olika områden, bl.a. inom EU. Olika myndigheter medverkar vidare i internationell samverkan som i regel har informationsutbyte som syfte. För att Sverige skall

få genomslag i sitt agerande på den internationella arenan bör det finnas en övergripande inriktning. Inriktningen bör också knyta an till och vara anpassad till respektive myndighets ansvarsområde.

Uppdraget

Den särskilda utredaren skall bedöma behovet av signalskydd i samhällsviktig verksamhet och lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall mot bakgrund av utvecklingen inom informationssäkerhetsområdet föreslå hur signalskyddstjänsten i Sverige skall vara organiserad. Utredaren skall också belysa hur signalskyddsutbildningen skall organiseras och var den skall lokaliseras.

Följande frågor bör besvaras.

- Hur bör signalskyddsverksamheten utvecklas så att den kan komma till nytta inom fler samhällssektorer?
- Vilka samhällssektorer har störst behov av signalskydd och vilka krav ställer de?
- Vem skall vara ansvarig för signalskyddet och hur skall detta vara organiserat?
- Vilka uppgifter skall signalskyddstjänsten ha och hur skall ledning och samordning ske?
- Hur säkerställs att det framtida behovet av kompetens inom det kryptografiska området kan tillgodoses?
- Hur säkerställs samordning med andra länders signalskyddsorganisationer på ett förtroendefullt och säkerhetsmässigt trovärdigt sätt?
- Hur åstadkoms en nationell distributionsfunktion för signalskyddsmateriel och signalskyddsnycklar för det internationella samarbetet?

Utredaren kommer att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas i framtiden. I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att genomföra (jfr. prop. 2001/2002:158).

Utredaren planeras också få uppdraget att genomföra den ovan nämnda utvärderingen.

Direktiv angående dessa två senare uppdrag avser regeringen att återkomma med under hösten 2002 som tilläggsdirektiv.

Samråd och avrapportering

Utredaren skall bedriva arbetet i nära samarbete med Försvarsmakten, Försvarets radioanstalt, Rikspolisstyrelsen och Krisberedskapsmyndigheten.

Inom Regeringskansliet finns en informell grupp bestående av representanter från Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet och Näringsdepartementet som utbyter information i dessa frågor. Denna grupp bör utredaren använda som referensgrupp i arbetet. Även andra kontakter bör tas.

Utredaren skall lämna delrapport om signalskyddstjänsten senast den 28 februari 2003.

Utredaren skall lämna slutrapport senast den 6 maj 2005.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2003:29

Beslut vid regeringssammanträde den 20 februari 2003

Sammanfattning av uppdraget

Utredningen angående vissa frågor om informationssäkerheten i samhället skall lämna förslag till hur den nationella strategin för informationssäkerhetsarbetetbör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas. I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) anmälde regeringen sin avsikt att göra en utvärdering av de bedömningar som regeringen gjorde inom informationssäkerhetsområdet. Utredaren skall följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit myndigheterna i uppgift enligt propositionen. Utredaren skall vidare lämna förslag till hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras.

Bakgrund

Med stöd av regeringens bemyndigande den 11 juli 2002 (dir. 2002:103) tillkallade chefen för Försvarsdepartementet en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall enligt direktiven lämna en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen angav i direktiven att den avsåg att återkomma med tilläggsdirektiv angående uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden.

OECD (Organisation for Economic Co-operation and Development) antog den 25 juli 2002 en rekommendation om nya riktlinjer

för nät- och informationssäkerhet (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). Riktlinjerna syftar till att stödja utvecklingen av en säkerhetskultur i samhället genom att främja säkerhetstänkande vid utveckling och användning av nät och informationssystem. Riktlinjerna innehåller mål och principer för utvecklingen av nya nät och informationssystem.

Uppdraget

En utvecklad svensk informationssäkerhetsstrategi

Utredaren skall i det fortsatta arbetet, utöver det tidigare lämnade uppdraget, även lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas. Den i prop. 2001/02:158 s. 103 redovisade strategin för informationssäkerhetsarbetet skall utgöra grunden.

Utredaren skall göra jämförelser med hur andra länder har hanterat informationssäkerhetsfrågan när det gäller strategi, organisation och andra förhållanden som kan vara relevanta.

I sitt arbete skall utredaren beakta OECD:s riktlinjer för nät- och informationssäkerhet och lämna förslag till hur riktlinjerna kan genomföras i utredarens förslag.

Följande frågor skall besvaras.

- Hur bör den nationella strategin för informationssäkerhet vidareutvecklas?
- Hur säkerställs att den nationella strategin för informationssäkerhet möter de krav som ställs via det multinationella samarbete Sverige deltar i, främst EU?
- Utifrån en nationell strategi behöver den nuvarande samordningen av Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet förändras?
- Inom vilka delar av informationssäkerhetsområdet bör staten ha ett särskilt ansvar?
- Hur skall informationssäkerhetsarbetet finansieras?

Utvärdering förutskickad i prop. 2001/02:158

I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) redovisade regeringen att de nya uppgifterna på informationssäkerhetsområdet skulle fördelas på de myndigheter som redan hade närliggande verksamhet. Regeringen anmälde också att man hade för avsikt att göra en utvärdering av denna fördelning av uppgifterna inom informationssäkerhetsområdet. Regeringen uteslöt inte att det skulle kunna finnas andra organisatoriska lösningar eller andra verksamheter inom informationssäkerhetsområdet som skulle kunna behövas ses över.

Som en förberedelse inför denna utvärdering skall utredaren skapa sig en god uppfattning av det ändamålsenliga i propositionens bedömningar att dela upp de nya uppgifterna genom att följa uppbyggnaden av verksamheten inom informationssäkerhetsområdet vid Krisberedskapsmyndigheten, Försvarets radioanstalt, Förvarets materielverk och Post- och telestyrelsen, inklusive den sistnämnda myndighetens uppdrag att inrätta en rikscentral för IT-incidentrapportering. Regeringen avser att återkomma till frågan om utvärderingen.

Författningsfrågor

Om utredaren finner att det finns ett behov av att föreslå författningsändringar skall utredaren lämna lagtekniskt genomarbetade förslag vid varje rapporteringstillfälle.

I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att låta genomföra (jfr. prop. 2001/02:158 s. 106).

I den mån det uppkommer frågor som rör behandling av personuppgifter skall de bestämmelser om skydd för den personliga integriteten vid behandling av sådana uppgifter som bl.a. finns i personuppgiftslagen (1998:204) och EG-direktivet om personuppgifter (95/46/EG) beaktas.

Utredningsarbetet

I sitt arbete skall utredningen ta hänsyn till OECD:s riktlinjer för nät- och informationssäkerhet.

Utredningen skall bedriva arbetet i nära samarbete med Rikspolisstyrelsen, Säkerhetspolisen, Datainspektionen, Statskontoret, Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk, Krisberedskapsmyndigheten, Totalförsvarets forskningsinstitut och Post- och telestyrelsen. Utredningen skall också ta de kontakter som behövs med viktiga IT-användare och andra intressenter, både inom den offentliga sektorn och i näringslivet, för att få en bild av vilka roller de spelar i informationssäkerhetsarbetet, deras behov och önskemål.

Utredningen skall utöver det som angavs i direktiven (2002:103) om att slutrapport skall lämnas senast 6 maj 2005 också lämna en delrapport angående uppdragen i detta tilläggsdirektiv senast den 1 mars 2004.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2004:46

Beslut vid regeringssammanträde den 7 april 2004.

Sammanfattning av uppdraget

Utredningen angående vissa frågor om informationssäkerheten i samhället skall genomföra den utvärdering som regeringen anmälde till riksdagen i proposition Samhällets säkerhet och beredskap (prop. 2001/02:158) vad avser de bedömningar som regeringen gjorde inom informationssäkerhetsområdet.

Bakgrund

Med stöd av regeringens bemyndigande den 11 juli 2002 (dir. 2002:103) tillkallade chefen för Försvarsdepartementet den 11 juli 2002 en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas. Utredaren lämnade en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen beslutade om tilläggsdirektiv för utredningen den 20 februari 2003 (dir. 2003:29) angående uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet för utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren fick också i uppdrag att följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit myndigheterna i uppgift enligt propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158). En delrapport skulle lämnas senast den 1 mars 2004.

I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) redovisade regeringen att de nya uppgifterna på informationssäkerhetsområdet skulle fördelas på de myndigheter som redan hade närliggande verksamhet. Regeringen anmälde också

att man hade för avsikt att efter två år göra en utvärdering av denna fördelning av uppgifterna inom informationssäkerhetsområdet. Regeringen uteslöt inte att det skulle kunna finnas andra organisatoriska lösningar eller andra verksamheter inom informationssäkerhetsområdet som skulle kunna behövas ses över.

Uppdraget

Utredningen skall genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) vad avser de bedömningar när det gäller uppgiftsfördelningen som regeringen gjorde inom informationssäkerhetsområdet. Utvärderingen skall redovisas i utredningens slutrapport senast den 6 maj 2005.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2005:53

Beslut vid regeringssammanträde den 28 april 2005.

Förlängd tid för uppdraget

Med stöd av regeringens bemyndigande den 11 juli 2002 tillkallade chefen för Försvarsdepartementet den 11 juli 2002 en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas (dir. 2002:103). Utredaren lämnade en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen beslutade om tilläggsdirektiv för utredningen den 20 februari 2003 (dir. 2003:29) med vilken utredningen gavs i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren lämnade en delrapport den 1 mars 2004.

Regeringen beslutade den 7 april 2004 om ytterligare tilläggsdirektiv till utredningen (dir. 2004:46) med uppdrag att genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) om den i propositionen redovisade uppgiftsfördelningen mellan myndigheterna inom informationssäkerhetsområdet. Utredningen skulle enligt direktiven redovisa sitt slutbetänkande senast den 6 maj 2005.

Utredningstiden förlängs, vilket innebär att utredaren skall redovisa sitt uppdrag senast den 9 september 2005. En delrapport skall lämnas den 6 maj 2005.

(Försvarsdepartementet)

Statens offentliga utredningar 2005

Kronologisk förteckning

1. Radio och TV i allmänhetens tjänst. Riktlinjer för en ny tillståndsperiod. Ku.
2. Radio och TV i allmänhetens tjänst. Finansiering och skatter. Ku.
3. Sveriges tillträde till 1995 års Unidroit-konvention om stulna eller olagligt utförda kulturföremål. Ku.
4. Liberalisering, regler och marknader. + Bilagor. N.
5. Postmarknad i förändring. N.
6. Säkert inlåst? En granskning av rymningarna från Kumla, Hall, Norrtälje och Mariefred 2004. Ju.
7. Försvarsfastigheter – information till riksdagen och effektiv lokalförsörjning. Fi.
8. Behov av rörlig ledningsstödsresurs. Fö.
9. KRUT Reformerat regelverk för handel med försvarsmateriel. UD.
10. Handla för bättre klimat. Från införande till utförande. M.
11. Välfärdsverksamhet för sjömän. N.
12. Bokpriskommissionens slutrapport. Det skall vara billigt att köpa böcker och tidskrifter. U.
13. Lördagsdistribution av dagstidningar. U.
14. Effektivare handläggning av anknytningsärenden. UD.
15. Familjeåterförening och fri rörlighet för tredjelandsmedborgare. UD.
16. Reformerat system för insättningsgarantin. Fi.
17. Vem får jaga och fiska? Rätt till jakt och fiske i lappmarkerna och på renbetesfjällen. Jo.
18. Prospektansvar. Fi.
19. Beskattningen vid omstruktureringar enligt fusionsdirektivet. Fi.
20. Konsumentskydd vid modemkapning. Ju.
21. Vinstandelar. Fi.
22. Nya upphandlingsregler. Fi.
23. en BRASkatt? – beskattning av avfall som förbränns. Fi.
24. Arbetslivsinriktad rehabilitering. Framtida organisation för Arbetslivstjänster och Samhall Resurs AB. N.
25. Gränslös utmaning – alkoholpolitik i ny tid. S.
26. Mobil med bil. Ett nytt synsätt på bilstöd och färdtjänst. + Bilaga, lättläst och Daisy. S.
27. Den svenska fiskerikontrollen – en utvärdering. Jo.
28. Dubbel bosättning för ökad rörlighet. Fi.
29. Storstad i rörelse. Kunskapsöversikt över utvärderingar av storstadspolitikens lokala utvecklingsavtal. Ju.
30. Lagen om byggfelsförsäkring. En utvärdering. M.
31. Stödet till utbildningsvetenskaplig forskning. U.
32. Regeringens stabsmyndigheter. Fi.
33. Fjärrvärme och kraftvärme i framtiden. M.
34. Socialtjänsten och den fria rörligheten. S.
35. Krav på kassaregister Effektivare utredning av ekobrott. Fi.
36. På väg mot ... En hållbar landsbygdsutveckling. Jo.

37. Tolkutbildning – nya former för nya krav. U.
38. Tillgång till elektronisk kommunikation i brottsutredningar m.m. Ju.
39. Skog till nytta för alla? N.
40. Rätten till mitt språk
    Förstärkt minoritetsskydd. Ju.
41. Bortom Vi och Dom.
    Teoretiska reflektioner om makt, integration och strukturell diskriminering. Ju.
42. Säker information. Förslag till informationssäkerhetspolitik. Fö.

Statens offentliga utredningar 2005

Systematisk förteckning

Jordbruksdepartementet

Vem får jaga och fiska?
Rätt till jakt och fiske i lappmarkerna och på renbetesfjällen. [17]
Den svenska fiskerikontrollen – en utvärdering. [27]
På väg mot ... En hållbar landsbygdsutveckling. [36]

Miljö- och samhällsbyggnadsdepartementet

Handla för bättre klimat.
Från införande till utförande. [10]
Lagen om byggfelsförsäkring.
En utvärdering. [30]
Fjärrvärme och kraftvärme i framtiden. [33]

Näringsdepartementet

Liberalisering, regler och marknader. [4]
Postmarknad i förändring. [5]
Välfärdsverksamhet för sjömän. [11]
Arbetslivsinriktad rehabilitering.
Framtida organisation för Arbetslivstjänster och Samhall Resurs AB. [24]
Skog till nytta för alla? [39]