InfoSäkutredningen

Denna broschyr summerar de viktigaste resonemangen och förslagen från InfoSäkutredningen, med särskilt fokus på de två delrapporterna Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) och Informationssäkerhetspolitik – organisatoriska konsekvenser (SOU 2005:71).

Syftet med att ge ut en sammanfattning, såväl på svenska som på engelska, är att uppnå större spridning av utredningens förslag och slutsatser samt att göra dessa tillgängliga i ett behändigare format. Betänkandena kan beställas i sin helhet från Fritzes Offentliga Publikationer (www.fritzes.se). De finns även tillgängliga I sin helhet på regeringens webbsida (www.regeringen.se).

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, till exempel 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 till exempel 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 inför, 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; att 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 delbetänkande tre 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, Samhällets säkerhet och beredskap) 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.

Utredningen föreslår 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 inför, 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 mellan privat och offentlig sektor

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 konstatera 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 (elförsörjning, telekommunkationer 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.

Idag 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 näringslivet och den offentliga sektorn.

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 Samhällets säkerhet och beredskap (prop. 2001/02:158) 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 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.

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 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.

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, till exempel 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 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 (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.

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

FHS 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.

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 inom det sjätte ramforskningsprogrammet har haft en budget på 3.600 miljoner Euro under fyra år. Inom Informationssamhällets teknik 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 KBM 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 (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 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 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.

Utredningens slutbetänkande Informationssäkerhetspolitik – organisatoriska konsekvenser (SOU 2005:71)

Frågor kring sårbarheten berör, som utredningen flera gånger påpekat, 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. Till detta måste läggas att bilden av dagens brister och hot är mycket komplex och därmed även behovsbilden.

Enligt utredningen är det viktigt att inse att det inte finns någon definitiv lösning på problemet med informationssäkerhet. Utredningen framhåller i Säker information – förslag till informationssäkerhetspolitik (2005:42) att en gemensam, nationell strategi och en samverkansprocess skulle kunna lära oss att leva med problem som rör informationssäkerhet. Detta förutsätter ett långsiktigt arbete mot övergripande, långsiktiga mål. Med det finns också behov av beslutskraft i ett kort perspektiv och en operativ förmåga för att kunna hantera incidenter i realtid. Därför behövs, enligt utredningen, en sammanhållen politik inom informationssäkerhetsområdet och en gemensam målstruktur.

I informationssäkerhet i Sverige och internationellt – en översikt (2004:32) redovisade utredningen en översikt av informationssäkerhetsarbetet i Sverige och internationellt. Utredningen kunde bland annat konstatera att även om problembilden i allt väsentligt sammanfaller, har länderna valt att organisera informationssäkerhetsarbetet på olika sätt. Det är således svårt att direkt överföra organisationsmodeller från ett land till ett annat.

I slutbetänkandet redovisar utredningen sina slutsatser och förslag till organisation av informationssäkerhetsarbetet i Sverige. De viktigaste utgångspunkterna återfinns i utredningens förslag till nationell strategi för ökad informationssäkerhet och i synen på omfattningen av det statliga åtagandet.

Den nationella strategin förutsätter organisatoriska grepp

Några av de förslag som redovisas i strategin förutsätter att staten utvecklar den egna organisationen och att samverkan mellan privat och offentlig sektor fördjupas. Behovet att förstärka informationssäkerhetsarbetet inom underrättelse- och säkerhetstjänsternas område, liksom att förstärka förmågan inom området nationell säkerhet, motiverar bland annat organisatoriska åtgärder. Inom båda dessa områden krävs, enligt utredningens mening, både tydligare ansvarsfördelning och säkerställande av kompetens och resurser.

Regeringen genomförde med början år 2002 organisatoriska förändringar för att etablera funktionerna omvärldsanalys, incidenthantering, teknikkompetens samt evaluering och certifiering. Den utvärdering som utredningen nu har gjort leder också till organisatoriska konsekvenser för berörda myndigheter.

Slutligen bör den av utredningen föreslagna strategin att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar i några fall leda till justeringar inom vissa myndigheter, utan att dessa behöver omorganiseras. Dessutom kan förutses att uppgifter i några fall bör preciseras och införas i berörda myndigheters instruktioner.

Det statliga åtagandet blir styrande

Statens åtagande, ansvar och intresse har av utredningen sammanfattats i fyra punkter (se ovan). Det statliga åtagandets omfattning leder till krav på att bygga upp förmåga inom flera viktiga områden och att lösa ett antal uppgifter i den statliga verksamheten. Informationssäkerhetsarbetet måste, som utredningen påpekar, utgöra en integrerad del av alla aktörers verksamheter, så också inom staten. Det följer av ansvarsprincipens tillämpning.

Utredningen redovisade även vad som bör falla inom det privata åtagandet och vad som skulle kunna betraktas som det statliga åtagandet, även om gränsdragningen är svår.

Enligt utredningens uppfattning bör även dessa åtaganden leda till organisatoriska konsekvenser. Utöver detta återstår att formulera nya uppdrag och uppgifter till myndigheter i den befintliga organisationsstrukturen, i syfte att öka informationssäkerheten.

Flera utgångspunkter för val av organisation

Utredningen har konstaterat att informationssäkerheten inte bara inrymmer frågeställningar för respektive verksamhetsansvarig, utan att det också finns problem av gemensam natur, där stora krav ställs på samordning. Vidare finns flera problem och frågeställningar av tvärsektoriell karaktär, som ofta kräver tillgång till specialistkompetens. Dessa problemområden förutsätter ett annat angreppssätt på styrning och organisation. Det är också viktigt att gränsdragningen mellan det privata och det offentliga åtagandet tydliggörs.

Vidare finns det, som utredningen redovisar under avsnittet om samverkan mellan privat och offentlig sektor, sannolikt frågeställningar som inte kan lösas av en aktör ensam, inte ens av staten. En fördjupad samverkan inom offentlig sektor och mellan privata och offentliga aktörer förutsätter en tydlig ansvarsfördelning inom staten och en organisation som kan hantera frågor av gemensam, tvärsektoriell natur i en vardag präglad av sektorstänkande och sektorsansvar.

Till dessa resonemang kan slutligen läggas att informationssäkerheten kräver tillgång till hög kompetens och resurser, såväl administrativt som tekniskt. I egenskap av liten

nation är det av synnerlig vikt att regeringen fokuserar de resurser som finns tillgängliga och utnyttjar samhällets samlade kapacitet på ett bättre sätt.

I tidigare betänkanden har utredningen pekat på ett antal förhållanden och synsätt som kan vara vägledande för informationssäkerhetsarbetet. Några av dessa är särskilt viktiga för val av organisation inom staten:

1. Informationssäkerhet omfattar hela samhället och frågeställningen är därför vidare än totalförsvarets behov.
2. Det finns ett behov att kraftsamla och att tydligare fokusera den statliga verksamheten nationellt, inom EU och internationellt.
3. Alla statliga aktörer måste, inom ramen för sitt respektive sektorsansvar, medverka till förmågan att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar.
4. Ansvaret för förmågan i den statliga kärnverksamheten, liksom för säkerheten i samhällsviktiga verksamheter, måste tydliggöras. Vissa gemensamma behov förutsätter bättre samordning inom staten och i samverkan med andra, icke-statliga aktörer.
5. Kompetensen och förmågan att hantera tvärsektoriella frågor måste säkerställas inom informationssäkerhetsområdet.

Tre grundläggande organisationsprinciper

Med de olika utgångspunkter som utredningen redovisar kan tre principer för organisation inom staten urskiljas.

Den första organisationsprincipen följer av ansvarsprincipen. Detta innebär att varje sektorsmyndighet har ansvaret för utvecklingen av informationssäkerheten inom sitt ansvarsområde och för de aktörer som berörs av myndighetens verksamhet. I syfte att tydliggöra omfattningen av detta ökade ansvar har utredningen i det tredje delbetänkandet lämnat ett förslag till förordning om vissa åtgärder för informationssäkerhet i den statliga verksamheten.[1] Inom några områden finns det enligt utredningens mening anledning att ytterligare tydliggöra detta ansvar och uppdrag. PTS utökade ansvar och befogenheter inom området elektronisk kommunikation är ett sådant exempel. Finansinspektionens samverkan med aktörer inom finansmarknaden är ett annat. I andra fall kan det handla om att ge

[1] Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42,) s. 31 ff.

ökad prioritet och lyfta upp säkerhetsfrågorna i berörda myndigheters verksamhet och förstärka insatserna, som exempelvis inom energi- och transportsektorn.

Den andra organisationsprincipen syftar till att tillgodose sådana behov som är gemensamma i den statliga verksamheten. Detta syftar framför allt till att uppnå en bättre samordning inom staten i administrativa och tekniska sammanhang

Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället, vare sig det handlar om att kunna hantera och ingripa vid störningar eller att ge underlag för förebyggande arbete hos alla aktörer.

Samverkan mellan privat och offentlig sektor

Genom tidigare betänkanden har utredningen visat att det finns sammanfallande problem och behov inom privat och offentlig sektor och att det finns anledning att samverka kring dessa, inte minst av praktiska skäl. Utredningen har vidare i sitt senaste delbetänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), konstaterat att det inte finns någon definitiv lösning på problemet med informationssäkerhet. En väl förankrad samverkansprocess skulle dock kunna lära oss leva med problemen.

Utredningen har därutöver funnit att det finns problemställningar som är av sådan art att ingen av aktörerna ensam kan klara av problemen. Följaktligen finns ett behov av att samverka för att identifiera och komma närmare lösningar på dessa. Det finns dessutom skäl att söka samverkan kring de prioriteringar som måste göras mellan olika problem och sektorer, i syfte att utnyttja tillgänglig kompetens och resurser på ett optimalt sätt.

Utredningens slutsats är att det i dagsläget finns en vilja till samverkan mellan aktörer i privat och offentlig sektor. Det är också utredningens uppfattning att näringslivet har ett intresse av att det finns adekvat utbildning, forskning och regelverk på informationssäkerhetsområdet. Den privata sidan kan bidra med tekniska lösningar och samhällets behov utgör en marknad för näringslivets aktörer. Det finns således en ömsesidig nytta i detta gemensamma intresse.

Företrädare för näringslivet har nu tagit ett initiativ till att bilda ett självständigt samverkansorgan. Detta bör därför tas tillvara av

staten, kommuner och landsting. Ett sådant organ bör, enligt utredningens mening, ha till uppgift att dels medverka till att öka medvetenheten i informationssäkerhetsfrågor, dels ge underlag för en lönsam och optimal riskhantering hos alla aktörer.

Utredningen föreslår att det redovisade samverkansinitiativet tas tillvara och att staten omgående utser en utredare eller förhandlare. I avvaktan på regeringens ställningstagande till utredningens övriga förslag, kan utredaren eller förhandlaren skapa underlag för ställningstagande till statens samverkan med andra aktörer inom informationssäkerhetsområdet samt klarlägga intresse och möjligheter för samverkan med kommuner och landsting i dessa frågor.

Regeringens ledande och samordnande roll

Regeringen har en ledande och samordnade roll inom informationssäkerhetspolitiken. Det sätt som regeringen väljer att sätta mål för verksamheter, styra och följa upp resultat är avgörande för myndigheternas arbete. Inom informationssäkerhetsområdet är det av särskild vikt med hänsyn till frågornas komplexitet, dynamik och internationella dimension. Utredningen återkommer därför till sitt förslag att utarbeta en sammanhållande målstruktur för informationssäkerhetsarbetet.

Utredningens utgångspunkter och slutsatser

Flera av de utgångspunkter som utredningen lyfter fram kan var och en för sig läggas till grund för val av organisation, med olika resultat beroende på vilka prioriteringar eller särintressen som styr valet. Den helhetssyn som enligt utredningen bör styra även valet av organisationslösning (och fördelningen av ansvar, befogenheter och skyldigheter inom staten) måste med nödvändighet bygga på en sammanjämkning av flera av de grundläggande frågeställningar som utredningen lyfter fram.

Tre grundläggande principer för organisation av informationssäkerhetsarbetet redovisas ovan. Den första följer ansvarsprincipen. Den andra syftar till att tillgodose gemensamma behov inom staten. Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället.

Mot denna bakgrund är utredningens första slutsats att det måste ligga inom varje myndighets ansvar att svara för informationssäkerheten i den egna verksamheten och i kontakt med de aktörer som berörs av myndighetens verksamhet. Detta följer av ansvarsprincipen. Ansvar, befogenheter och skyldigheter bör förtydligas i berörda myndigheters instruktioner och i regleringsbrev. Föreskrifter samt råd och anvisningar bör utarbetas till den av utredningen föreslagna förordningen om vissa åtgärder för informationssäkerhet hos staten.

Utredningen föreslår att informationssäkerhetsarbetet bör organiseras så att kraftsamling kan ske till administrativa respektive tekniska frågeställningar. Utredningens andra slutsats är därför att gemensamma behov inom staten och tvärsektoriella frågeställningar i hela samhället bör samlas under en myndighet för administrativa funktioner respektive en myndighet för tekniska funktioner. Därmed förbättras även förutsättningarna för en sammanhållen informationssäkerhetspolitik.

Utredningens tredje slutsats är att några myndigheter, inom ramen för sina nuvarande ansvarsområden, bör ges utökade uppgifter och resurser för förebyggande arbete, rådgivning med mera.

Utredningen har visat att det finns problemställningar, som är av sådan art, att ingen av samhällets aktörer ensam kan lösa dem. En fjärde slutsats är därför att samverkan mellan privat och offentlig sektor bör utvecklas på informationssäkerhetsområdet.

Slutligen framhåller utredningen regeringens ledande och samordnande roll. Utredningens femte slutsats är att denna roll i informationssäkerhetsarbetet förutsätter en sammanhållande målstruktur som även fångar in frågeställningar som rör gemensamma och tvärsektoriella problem.

En ny organisationsstruktur för informationssäkerhetsarbetet

Ansvaret för policyfrågor och den administrativa funktionen, liksom ansvaret för den tekniska funktionen skulle kunna samlas i en central myndighet för informationssäkerhet. Utredningen har dock stannat för att föreslå att KBM förstärks och ges samordningsansvaret för policy och administrativ informationssäkerhet. Samordningsansvaret för den tekniska informationssäkerheten föreslås läggas på en nybildad myndighet med ansvar för signalunderrättelser, signalskydd och hög

teknikkompetens. Denna nya myndighet föreslås huvudsakligen bygga på den kompetens som i dag finns inom FRA men med utökat ansvarsområde och förstärkta resurser. Den föreslagna förändringen motiverar också ett nytt namn som bättre återspeglar dess uppgifter än vad namnet Försvarets radioanstalt gör. Utredningen föreslår namnet Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet (IST).

Motivet för två myndigheter med samordningsansvar för olika delar av informationssäkerheten är framför allt att det är rationellt och ger utrymme för synergieffekter med dessa myndigheters övriga ansvarsområden. Det bör ge underlag för en bättre sammanhållen informationssäkerhetspolitik. Detta förutsätter dock ett välutvecklat löpande samarbete mellan de båda huvudansvariga myndigheterna, liksom mellan dessa och andra myndigheter, näringslivet och andra aktörer som har uppgifter och behov på informationssäkerhetsområdet.

Utredningens förslag kommer att få vissa konsekvenser för berörda myndigheters personal. I flera fall föreslår utredningen en förstärkning av kompetens och bemanning. De medel som hittills anslagits som projektmedel för informationssäkerhet via den så kallade civila ramen föreslås omvandlas till ordinarie anslagsmedel. Det innebär samtidigt en markering av att myndighetsorganisationen för informationssäkerhet får en permanent karaktär, efter de inledande årens mera projektinriktade uppbyggnadsperiod.

Det utökade ansvaret för informationssäkerhet som utredningen föreslår bör också återspeglas på ledningsnivå i de båda myndigheter som föreslås få samordningsansvar.

Policyansvar och administrativt samordningsansvar

I policyansvaret ligger att förvalta och utveckla den nationella informationssäkerhetsstrategin, att samordna informationssäkerhetsarbetet mellan samhällets aktörer, att under regeringen inrikta samhällets informationssäkerhetsarbete, att utgöra samhällets kontaktpunkt för informationssäkerhet och att under regeringen utgöra internationell kontaktpunkt genom att samordna och där så bedöms lämpligt företräda Sverige i internationell samverkan, där inte andra myndigheter är utpekade.

Också nationellt har utpekandet av en samordnande myndighet betydelse för allmänhet, näringsliv, kommuner etc. Det underlättar

för samtliga aktörer i samhället om de i policyfrågor kan vända sig till en myndighet med frågor som rör informationssäkerhet eller skyddet av samhällsviktig IT-infrastruktur. Detta innebär i sig inget avsteg från ansvarsprincipen eftersom genomförandet av specifika uppgifter även fortsättningsvis bör ligga hos direkt ansvariga myndigheter.

KBM bör i sin roll som policymyndighet ges möjlighet att ge ut föreskrifter om en grundläggande säkerhetsnivå med stöd av den av utredningen föreslagna förordningen om informationssäkerhet hos staten.[2] Nära samverkan måste härvidlag etableras med sektorsansvariga myndigheter med egen föreskriftsrätt, exempelvis PTS, Finansinspektionen samt Säkerhetspolisen.

Även revision och tillsyn av föreskrifterna måste utvecklas. Detta bör dock genomföras av annan aktör än KBM, exempelvis av Statskontoret i en ny roll.

KBM sammanställer en helhetsbild genom sitt utpekade ansvar för omvärldsanalys. Denna kan i en förändrad organisation utvecklas ytterligare, bland annat genom att KBM får en förbättrad tillgång till underrättelserapporter.

Det finns behov av en formaliserad samverkan med KBM som samordnande myndighet mellan aktörer i samhället som äger, driver, eller på annat sätt har ansvar för samhällsviktig verksamhet eller infrastruktur. Informationsutbytet kan avse incidenter, bästa metod, hotbilder, risker och sårbarheter. Informationen måste fungera både inom, respektive mellan, stat, kommuner, näringsliv och andra organisationer.

Samverkan ger ett viktigt underlag till helhetsbilden liksom den till ömsesidig nytta förmedlar känslig eller förtrolig information, frågeställningar och påverkan. Det innefattar också till exempel att delta i och analysera utvecklingen inom EU och i övriga internationella sammanhang och att delta i relevanta arbetsgrupper för att strategiskt påverka de processer inom EU och internationellt som berör Sverige. Samverkan bidrar också till att stärka Sveriges position i dessa aktiviteter.

KBM bör i extraordinära situationer ha ett delegerat ansvar att inom givna ramar samordna informationssäkerhetsarbetet.

Utifrån helhetsbilden och policyansvaret på informationssäkerhetsområdet samt utifrån KBM:s befintliga kompetens på övningar på krishanteringsområdet är det naturligt att KBM har det samordnande myndighetsansvaret för övningar på

[2] Förslag till förordning om vissa åtgärder för informationssäkerhet hos staten. Se Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), sid. 31ff.

informationssäkerhetsområdet. Liksom i det förebyggande arbetet kan övningsverksamheten till stor del hanteras av näringslivet. KBM:s roll bör främst vara att identifiera, uppmärksamma och formulera behov och mål för insatserna.

Det förefaller naturligt att samordning av kontakter mellan privat och offentlig sektor faller på KBM inom ramen för myndighetens samordningsansvar.

Signalskyddsutbildning

Utredningen förordar en signalskyddstjänst som omfattar hela samhällets behov, inte bara totalförsvarets. För att skapa möjlighet till helhetssyn för den utbildning som erfordras inom informationssäkerhetsområdet samt för att uppnå synergieffekter bör signalskyddsutbildningen utvecklas så att utbildning kan ges inom hela informationssäkerhetsområdet. Utredningen föreslår därför att huvudmannaskapet för signalskyddsutbildningen överförs från Försvarsmakten till KBM.

Tekniskt samordningsansvar

Utredningen föreslår att ansvaret för signalskydd överförs från Försvarsmakten, MUST Säkerhetskontor, till den nybildade myndighet, IST, som övertar FRA:s nuvarande uppgifter. Även KBM:s ansvar för nyckeldistribution föreslås överföras till IST. Det administrativa godkännandet av signalskyddssystem, liksom även föreskriftsrätten för samhällsviktiga system, föreslås dock placeras vid KBM.

KBM:s signalskyddsverksamhet bedrivs i huvudsak i Sollefteå. Överföringen bör leda till en utökad bemanning av signalskyddsverksamhet i Sollefteå.

Utöver det nuvarande signalspaningsuppdraget har FRA uppgifter inom svensk informationssäkerhet. Det gäller kompetens inom kryptologi, där FRA sedan 1980-talet svarar för att bemanna de kryptologiska funktionerna vid MUST.

FRA har också sedan 2003 en särskild teknikkompetensfunktion, TKF, till stöd för statliga myndigheter och bolag, som bland annat medverkar i tester av säkerheten i myndigheters IT-system tillsammans med berörda myndigheter. Informationssäkerhetsuppgifterna har tillförts FRA för att

nyttiggöra FRA:s unika signalspaningskompetens och allmänt höga tekniska kompetens. FRA har färdiga krisberedskapsprocesser som har testats och används i verkliga fall för att stödja insatser vid myndighetskriser. Dessa kommer att vara värdefulla om det skulle uppstå en nationell kris med IT-inslag.

Signalskydd och signalspaning kan ses som två sidor av samma mynt. Det finns fördelar med ett nära samarbete mellan dessa båda områden. Länder med brister i signalskyddet har ofta dålig kontakt mellan signalskydd och signalspaning. Det behövs kompetens i att forcera bristfälligt signalskydd för att kunna skapa ett eget bra signalskydd. Kompetensen härför finns för närvarande i första hand inom FRA.

Svensk kryptoindustri har idag svårt att konkurrera med utländsk, då det inte finns en inhemsk organisation som kan godkänna kryptosystem utanför totalförsvaret. Det visar på ytterligare ett behov av att bredda omfattningen av samhällets signalskydd, vilket kan ske genom en flyttning av signalskyddsfunktionen, från Försvarsmakten till den nybildade myndigheten för teknisk informationssäkerhet, IST. Den enda icke-militära myndighet som är aktuell är FRA. Verksamheterna för nyckelproduktion och signalkontroll skulle därmed kunna integreras, eftersom dessa redan finns inom nuvarande FRA.

En effekt som uppstår vid samordning av alla teknikdelar hos en myndighet är snabbare beslutsvägar. Det är av stor vikt att snabbt kunna sätta ihop en insatsgrupp för att stödja insatser vid nationella kriser med IT-inslag och för att kunna medverka till identifiering av inblandade aktörer i IT-relaterade hot mot samhällsviktiga system. Med en delad organisationsbild är det svårare att upprätthålla en kritisk kompetensmassa.

Om uppgiften att leda och samordna signalskyddstjänsten inom totalförsvaret överförs från Försvarsmakten, erfordras att de medel som finns avsatta i materielplanen för utveckling också förs över. Försvarsmakten kommer oavsett vem som har det samordnande ansvaret för signalskyddstjänsten att vara en av de största avnämarna.

Sverige har på senare år deltagit alltmer aktivt i internationella signalskyddssammanhang. För att det internationella arbetet skall vara väl koordinerat behövs en utpekad National Communications Security Agency (NCSA), det vill säga en organisation i landet som ansvarar för signalskyddsfrågor, och en National Distribution Agency (NDA), en organisation som är behörig att distribuera kryptonycklar. Utredningen föreslår att den nybildade

myndigheten för teknisk informationssäkerhet, IST, ges uppgifterna som NCSA och NDA.

Incidentrapporteringsfunktion

Sveriges IT-incidentcentrum, Sitic, vid Post- och telestyrelsen ansvarar för systemet för informationsutbyte om IT-incidenter mellan samhällets alla aktörer. Uppgiften är bland annat att snabbt sprida information om IT-incidenter, att lämna information och råd om förebyggande åtgärder, att sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

Om Sitic skall fungera väl krävs ett nära och förtroendefullt samarbete med andra aktörer inom informationssäkerhetsområdet, inte minst med KBM och den nya myndigheten IST, som föreslås få särskilt samordnande uppgifter för den nationella informationssäkerheten. Det är angeläget att sådana väl fungerande samarbetskanaler finns såväl på ledningsnivå i myndigheterna, som på handläggarnivå.

Certifiering och evaluering

Det nationella systemet för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med IS 15408 Evalueringskriterier för IT-säkerhet i produkter och system (Common Criteria) tillkom efter riksdagens beslut under 2002. Certifieringsorganet är nu etablerat som en oberoende funktion inom FMV med namnet Sveriges Certifieringsorgan för IT-säkerhet, CSEC.

Arbetet med att etablera certifieringsordningen är genomfört. Detta arbete omfattar bland annat utarbetande av kvalitetsmanual, ansvarsbeskrivningar, beskrivningar av processer för licensiering av evalueringslaboratorier, regler för genomförande av certifieringar samt utbildning av certifierare och evalueringsföretag.

Utredningen finner att de motiv som anfördes inför riksdagsbeslutet om etableringen av ett svenskt system för evaluering och certifiering alltjämt är giltiga. Utredningen har också i tidigare betänkanden betonat vikten av att tillämpa existerande internationella standarder inom IT-säkerhetsområdet. Common Criteria syftar till att sammankoppla ledningsfunktioner,

inklusive riskhantering, och mer detaljerade tekniska specialstandarder med hur krav på säkerhets- och skyddsfunktioner ska kunna härledas, uttryckas och verifieras i de tekniska lösningarna i IT-produkter och program.

Utredningen föreslår att uppgiften som signatär inom ramen för CCRA överförs från Swedac till KBM. Swedacs uppgifter och roll för ackreditering och teknisk kontroll för andra, öppna system inom till exempel EU föreslås oförändrad.

Frivillig krisresurs

Ett sätt att bidra till att kunna hantera en allvarlig eller extraordinär situation vore att mobilisera kompetens dit den behövs, för att begränsa en skada eller att arbeta förebyggande mot nya attacker eller angrepp. Ett sådant nationellt säkerhetsinitiativ skulle vara att upprätta en kompetensbank. Det samordnande ansvaret för att ta tillvara sådana frivilligresurser bör läggas på KBM som ges uppgiften att hantera kontakterna och upprätta erforderliga avtal med enskilda och berörda företag samt tillse att övningsverksamhet genomförs.

Rikspolisstyrelsen och Statens kriminaltekniska laboratorium

Allvarliga IT-incidenter utgör i grunden ofta brott. Inom informationssäkerhetsområdet har det visat sig att en rad myndigheter och andra organisationer har behov av polisens medverkan i olika arbets- och samverkansgrupper. Polisen och Säkerhetspolisen kan genom sina operativa uppdrag tillföra erfarenheter inom området.

Rikskriminalpolisen är Sveriges kontaktpunkt inom ramen för G8:s 24/7 High Tech Crime arrangemang och Interpols National Central Reference Point System , NCRP, vilket understryker att polisen är en viktig aktör i samhällets informationssäkerhetsarbete.

För att möta dessa omvärldskrav och ett önskemål om samordning internt inom polisen, har en för Rikskriminalpolisen och Säkerhetspolisen gemensam funktion, S-BIT, etablerats. Då verksamheten inte fått öronmärkta medel för området har funktionen endast ett begränsat antal tjänster, mot planerade 12. För att leva upp till de beskrivna målen och de krav och önskemål som ställs på polisen inom området informationssäkerhet är det

önskvärt att särskilda medel kan avsättas för ändamålet. S-BIT:s verksamhet bör därför delvis finansieras med medel ur KBM:s så kallade civila ram eller genom anslagstilldelning.

Allt större del av den brottsutredande verksamheten kommer i kontakt med IT och kräver kunskaper om bevissäkring och undersökning i IT-miljö, så kallad IT-forensisk verksamhet. Inom det IT-forensiska området och vid vissa tekniska problem, lämnar FRA i vissa fall stöd till polisen. Det är av vikt att metodutvecklingen vad gäller IT-forensisk verksamhet sker inom polisen, i första hand vid Statens kriminaltekniska laboratorium (SKL). Den nybildade myndigheten IST bör dock kunna vara en stödjande resurs, särskilt ifråga om kryptologisk kompetens.

Ekonomiska konsekvenser

Utredningens förslag innebär en höjd ambitionsnivå för samhällets informationssäkerhet. Vissa av förslagen medför ökade kostnader. Det gäller dels ökade resursbehov vid KBM, dels vid den nybildade myndigheten, IST, som föreslås få policyansvar och administrativt samordnande ansvar respektive tekniskt samordnande ansvar för samhällets informationssäkerhet.

Vidare föreslås att finansieringen av Sitic, Sveriges incidenthanteringscentrum, vid Post och telestyrelsen och CSEC , Sveriges Certifieringsorgan för IT-säkerhet, skall ske via ordinarie anslag.

Finansiering föreslås ske genom avräkning från KBM:s så kallade civila ram, 7:5 Krisberedskap. Efter avräkning kvarstår ett ökat anslagsbehov med 43 miljoner kronor per år för att kunna genomföra utredningens förslag till förbättrad informationssäkerhet.

Utredningen föreslår vidare överflyttning av ansvar och verksamhet för signalskydd från Försvarsmakten, MUST Säkerhetskontor, till den nybildade myndigheten för teknisk informationssäkerhet, IST. Även KBM:s ansvar och verksamhet för signalskydd föreslås överflyttat till IST. Det administrativa godkännandet av signalskyddssystem föreslås dock placeras vid KBM. Utredningen föreslår också en överföring av huvudmannaskapet för signalskyddsutbildningen från Försvarsmakten till KBM. Förslagen avses ej få kostnadseffekter för statsbudgeten.

Utredningen har också i sitt tidigare betänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) föreslagit att KBM genom sin roll i forskningshänseende bör utveckla ett tematiskt forskningsområde kring informationssäkerhet. För att en satsning skall uppfattas som meningsfull inom forskarsamhället bör den årliga ramen vara 10-15 miljoner kronor, beroende på medfinansiering. Finansieringen av KBM:s insats i en sådan satsning föreslås ske via projektmedel ur den civila ramen.