Informationssäkerhet i Sverige och internationellt

– en översikt

Delrapport 2 från InfoSäkutredningen

Stockholm 2004

STATENS OFFENTLIGA UTREDNINGAR

SOU 2004:32

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 kan beställas hos:
Information Rosenbad
Regeringskansliet
103 33 Stockholm
Fax: 08–405 42 95
Telefon: 08–405 47 29
www.regeringen.se/propositioner/sou/pdf/remiss.pdf

Tryckt av Edita Norstedts Tryckeri AB
Stockholm 2004

ISBN 91-38-22108-X
ISSN 0375-250X

Missiv

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).

En delrapport om signalskydd lämnades till regeringen den 28 februari 2003.

Utredningens uppdrag utökades genom tilläggsdirektiv beslutade den 20 februari 2003 (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 skall dessutom följa myndigheternas uppbyggnad av de verksamheter som regeringen aviserade i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158) angående informationssäkerheten i samhället.

Med anledning av det utökade uppdraget tillkom experter samt två sakkunniga. Som ytterligare experter utsågs den 28 maj 2003 övers-

telöjtnant Håkan Gustafsson, avdelningschef Anders Johanson, säkerhetschef Bo Karlsson, enhetschef Staffan Karlsson, överingenjör Mats Ohlin, doktorand Anna Palbom, avdelningsdirektör Anna-Karin Waldton samt avdelningsdirektör Wiggo Öberg och som sakkunnig departementssekreterare Julia Mikaelsson. Kansliråd Ulf Johansson och ämnessakkunnig Richard Oehme kvarstår som sakkunniga och ämnessakkunnig Helena Lindberg (entledigad från den 1 september 2003), chefsjurist Elisabeth Lager, avdelningschef John Daniels, signalskyddssamordnare Arne Jonsson och avdelningsdirektör Kristina Starkerud som experter. Kansliråd Fredrik Sand förordnades som sakkunnig från och med den 2 november 2003.

I det fortsatta arbetet har departementsrådet Michael Mohr fungerat som huvudsekreterare och Josefin Grennert och Anja Stegen som sekreterare.

Utredningen har antagit namnet InfoSäkutredningen.

Arbetssätt och förankring

En informell grupp inom Regeringskansliet som utbyter information om informationssäkerhetsfrågor har beretts möjlighet att delta i utredningens arbete. Gruppen består av representanter från Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet, Finansdepartementet och Näringsdepartementet. Förankring i den privata sektorn har skett genom möten i samarbete med organisationen Svenskt Näringsliv, där ett stort antal företrädare från branschorganisationer och företag deltagit vid möten och lämnat skriftligt underlag och synpunkter.

Utredningen har genomfört besök och intervjuer vid verksamheter med koppling till informationssäkerhet för att få en bild av läget i Sverige, och för att identifiera problemområden inom detsamma. Kontakter med företrädare för näringslivet har också tagits. En dialog med berörda myndigheter och organisationer har upprätthållits under hela arbetet. Ett försök att beskriva de olika departementens roller inom informationssäkerhetsarbetet har också genomförts. För att få en oberoende bild av förutsättningar och begrepp inom informationssäkerhetsarbetet, har utredningen för detta arbete anlitat en konsult, Bo Riddarström på BRi Konsult AB. Åke Pettersson, tidigare särskild utredare i Sårbarhets- och

son, tidigare särskild utredare i Sårbarhets- och säkerhetsutredningen, har fungerat som resursperson för utredningen, särskilt vad avser frågor rörande kompetensförsörjning.

Utredningen har sedan delbetänkande 1 den 28 februari 2003 genomfört studieresor till Frankrike, Norge, Tyskland och Storbritannien.

Avgränsning och ambition med delbetänkande 2

Utredningen konstaterade i delbetänkande 1 om Signalskydd att IT-säkerhet och signalskydd som traditionellt har hanterats som två separata verksamheter idag inte kan separeras vare sig konceptuellt eller i praktiskt arbete. Signalskydd kommer därför i utredningens fortsatta arbete att betraktas som en integrerad del av informationssäkerheten.

Ambitionen inför delbetänkande 2 från utredningen är att presentera en bland relevanta aktörer förankrad bild av informationssäkerhetsarbetet i Sverige i dag. Detta omfattar såväl påbörjat och planerat arbete, som gällande förutsättningar och begrepp inom området. Materialet skall användas som avstamp för vidare arbete med att formulera en välgrundad och genomförbar strategi för utvecklingen av informationssäkerhetsarbetet. Utredningen har gjort bedömningen att detta är ett nödvändigt steg för att kunna förhålla sig till eventuella meningsskiljaktigheter och missförstånd gällande språkbruk som finns inom området. Genom en inblick i och förståelse för det arbete som idag bedrivs har utredningen ambitionen att i ett senare skede kunna lämna förslag på annan ordning eller kompletterande snarare än överlappande verksamhet.

Som en grund för framtida förslag, presenterar utredningen även i denna delrapport en övergripande beskrivning av den internationella utvecklingen på informationssäkerhetsområdet. En mer utförlig beskrivning av informationssäkerhetsarbetets utveckling inom EU lämnas, där även den legala begreppsapparaten beskrivs. Utredningen bedömer att detta är en viktig grund för det fortsatta arbetet och utvecklingen av informationssäkerheten i Sverige.

Under arbetets gång har utredningen uppmärksammat betydelsen av kompetensförsörjning inom informationssäkerhetsområdet, var-

för detta i denna delrapport har getts ett större utrymme än ursprungligen var tänkt. Utredningen avser att även i det fortsatta arbetet lägga stor vikt vid dessa frågor.

Stockholm 1 mars 2004

Anders Svärd

/Michael Mohr
Josefin Grennert
Anja Stegen

Innehåll

1 Utgångspunkter för informationssäkerhet

Sverige skall, i enlighet med det IT-politiska beslutet som fattades 2000, vara världsledande i användandet av informationsteknik (IT). IT utgör en viktig förutsättning för tillväxt och utveckling. Detta förutsätter en tillit till systemen och att den information som flödar i systemen är tillförlitlig. Informationssäkerhet är därmed en viktig förutsättning som bör utgöra en integrerad del av utbyggnaden av informationssamhället.

I detta avsnitt ges en inledande beskrivning av utvecklingen av ett antal centrala begrepp och definitioner inom informationssäkerhetsområdet, och vilka utgångspunkter utredningen tar i denna rapport.

För att illustrera över vilket brett spektrum informationssäkerhetsfrågorna spänner, och av vilken betydelse god informationssäkerhet är, nämns nedan några belysande exempel[1]:

Exempel 1: Ett litet, högteknologiskt företag som utvecklar programvara för styrning av industriprocesser har mycket av sina värden lagrade i form av programkod (information). Om företaget inte har genomfört nödvändiga IT-säkerhetsåtgärder kan dessa värden lätt förloras, t.ex. genom att en hackare förstör koden eller att en anställd stjäl koden. Sker något av detta måste företaget lägga ner stora resurser på att återskapa den förstörda eller stulna informationen.

Exempel 2: Avbrott i kraftförsörjningen kan vara mycket kritiskt för de flesta verksamheter. Driftskontrollsystem i dagens kraftförsörjning är i stor utsträckning baserad på fjärrstyrning, där IT-system har en central roll. Sådana system baseras gärna på öppet

[1] Exemplen är hämtade från den norska strategin för informationssäkerhet.

tillgängliga standarder och det är enkelt att integrera dem med administrativa system hos kraftleverantörerna. Detta ger utvidgad funktionalitet och effektivitet. Administrativa system knyts gärna mot publika nät, något som kan exponera driftkontrollsystem, och därmed driften av kraftförsörjningen, för risker som en sådan nätuppkoppling kan föra med sig. Bristande säkerhetsåtgärder och/eller tillräcklig kompetens hos en ondsint aktör kan därför skada driftkontrollsystemet. Sådana avbrott i kraftförsörjningen kan få allvarliga samhälleliga konsekvenser.

Exempel 3: Överföring av ljud, text, bilder och andra data med hjälp av elektromagnetiska signaler kräver tillgängliga och säkra kommunikationsnät. Brott i kablar, radioutrustning, och liknande kan få stora konsekvenser både för leverantörerna och användarna av elektroniska kommunikationstjänster. Angrepp riktade mot dessa system kan därför få allvarliga samhälleliga konsekvenser.

Våra publika nät, som t.ex. mobilnät, är inte dimensionerade så att alla kan använda dessa samtidigt. I en situation med onormalt mycket trafik kan mobilnäten därmed bli överbelastade så att användarna inte kan utnyttja tjänsterna. Genom att störa mobilnäten, som många har gjort sig beroende av, kan liv och hälsa riskeras. Därutöver får långvarigt bortfall av kommunikation stora ekonomiska konsekvenser.

Exempel 4: En läkare som skall skicka en journal elektroniskt måste ha en teknisk lösning på sin klinik som beaktar informationssäkerheten. Mottagaren måste vara säker på att det är en auktoriserad läkare och att det är den rätte läkaren som skickar journalen. Det måste också gå att vara säker på att informationen i meddelandet är korrekt och inte har blivit manipulerad på vägen. Sist men inte minst måste informationens konfidentialitet vara betryggande. Utan sådana säkerhetsåtgärder är elektronisk överföring av journaler varken försvarbara eller möjliga.

Exempel 5: När en privatperson använder bank via Internet på en hemdator, som också andra använder för att kommunicera på nätet med, skall denna person vara medveten om vilka hot som informationen lagrad i datorn kan utsättas för. Har datorn bredbandsuppkoppling till Internet kan den stå öppen för angrepp utifrån om den inte är försedd med korrekt installerad och uppdaterad brandväggstjänst, vilket ofta är svårt att åstadkomma för en mindre van

privatperson. Samma dator kan också användas för att angripa andra användare av nätet, utan att ägaren är medveten om det. Därför är det viktigt också för privatanvändare att ha goda rutiner för användandet av datorn, dvs. skilda användarområden, kontroll av lagringsmedier, kontroll av nättillgång osv.

1.1 Begrepp och definitioner

Dagens begrepp och definitioner har vuxit fram i takt med utvecklingen av de tekniska och funktionella förutsättningarna inom IT-området. De har huvudsakligen formulerats av inblandade aktörer efter egna specifika behov. Framväxten av begrepp och definitioner kan därför i stort sett sägas ha skett ur ett underifrånperspektiv.

Till statsmakternas uppgift hör att formulera spelregler på övergripande nivå, dvs. legala, administrativa eller finansiella regler som ger förutsättningar för politiskt beslutade mål t.ex. tillväxt, konkurrens och välfärd. Dessa spelregler är övergripande och har därför ofta formulerats ur ett ovanifrånperspektiv.

Tidsperspektiven skiljer sig mellan aktörerna. Lagstiftaren har ett utpräglat långt perspektiv vilket därmed kan medföra svårigheter att alltid vara uppdaterad. Branschens aktörer och användare har av naturliga skäl ett kortare tidsperspektiv.

Lagbestämmelser om informationssäkerhet finns idag endast i Säkerhetsskyddslagen (1996:627) och har där ett definierat men avgränsat syfte (se vidare kapitel 3). Utredningens utgångspunkt är att informationssäkerhet måste ses i ett bredare sammanhang. Det faktum att en mycket stor del av informationshanteringen i samhället inte längre föreligger i fysisk form återspeglas dåligt i befintliga regelverk. Begrepp och definitioner är allmänt hållna. Liksom i de flesta andra länder finns det dessutom luckor i den nationella lagstiftningen. Mot denna bakgrund är det enligt utredningens mening viktigt att finna bättre begrepp och definitioner som rör informationssäkerheten.

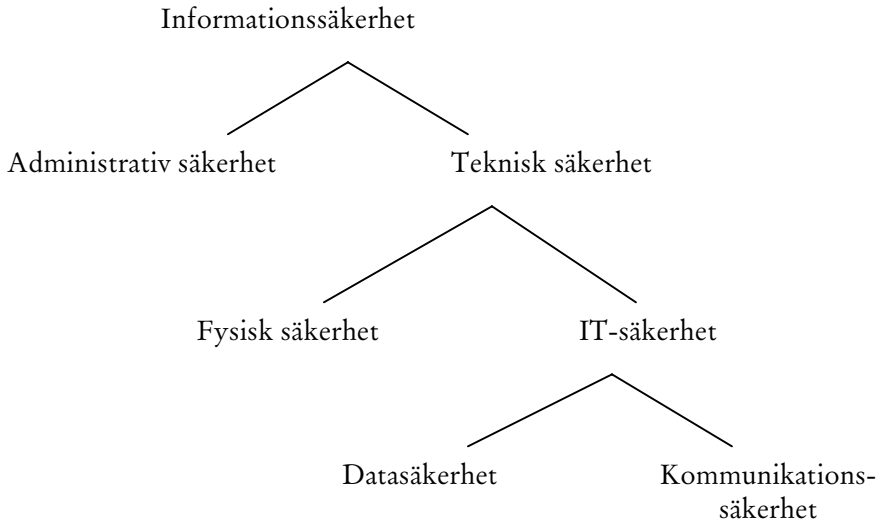
1.1.1 Ledningssystem för informationssäkerhet

Den svenska standarden SS-ISO/IEC 17799 respektive SS 62 77 99 avseende Ledningssystem för informationssäkerhet, vars två delar utgör dels riktlinjer för ledning av informationssäkerhet, dels specifikation med vägledning för användning, innehåller väl inarbetade begrepp och definitioner inom informationssäkerhetsområdet.

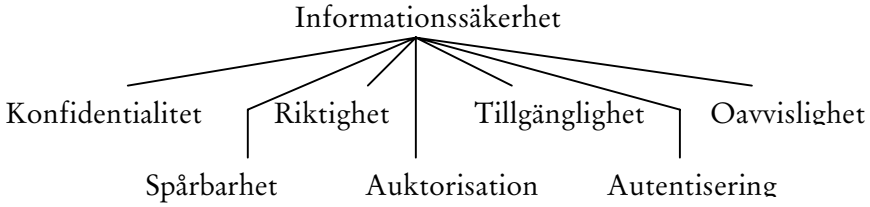
1.1.2 Standardiseringen i Sverige (SIS)

I SIS tekniska rapport Handbok 550: Terminologi för informationssäkerhet (2003) sammanfattas rådande uppfattning i fråga om vissa begrepp och definitioner. Enligt SIS arbetsgrupp innefattar begreppet informationssäkerhet ett brett område av termer som rör allt från grundläggande policy, via riskhantering och administrativa till tekniska åtgärder och mekanismer.

Informationssäkerhet kan således beskrivas på flera olika sätt, beroende på ändamål. En uppdelning som redovisas i SIS-rapporten (figuren nedan), utgår från skyddsåtgärdernas miljö, teknisk respektive administrativ säkerhet etc. Administrativ säkerhet omfattar bl.a. metoder, regelverk, organisation, utbildning och kontroll.



Ett annat sätt att dela upp begreppen kan vara utifrån infologiska skyddsmål. En vanlig uppdelning kan vara följande:



1.1.3 Basnivå för IT-säkerhet (BITS)

Krisberedskapsmyndigheten (KBM) lämnar, i form av 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. Till dessa rekommendationer föreslås ett antal begrepp och definitioner. Dessa följer i huvudsak SIS-rapportens, men lägger större vikt vid andra begrepp som t.ex. systemägare.

1.1.4 EU och informationssäkerhet

Sedan 1990-talet finns ett antal direktiv, meddelanden och förslag inom EU som berör informationssäkerhet. Av särskilt intresse för utredningen är Europeiska unionens råds beslut om säkerhetsbestämmelser och rambeslut om angrepp mot informationssystem, som båda innehåller ett antal begrepp och definitioner för gemenskapen. Informationssäkerhetsarbetet inom EU redovisas närmare i kapitel 4.

1.1.5 Informationsoperationer

Informationskrigföring (IW) och informationsoperationer (IO) är omdiskuterade begrepp med varierande innebörd. Språkbruk och definitioner skiljer sig åt mellan olika länder. På senare år har informationskrigföring i många sammanhang kommit att ersättas av det vidare begreppet informationsoperationer. Informationsoperationer brukar användas för att beskriva samlade och samordnande åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. Det kan ske genom att utnyttja egen information och egna informationssystem samtidigt som dessa måste skyddas. Det finns både offensiva och defensiva informationsoperationer. De kan genomföras i politiska, ekonomiska och militära sammanhang. Den främsta defensiva komponenten inom informationsoperationer brukar benämnas informationssäkring. Informationsoperationer utgår från ett säkerhetspolitiskt perspektiv och fokuserar på stater eller andra säkerhetspolitiska aktörer.

1.1.6 Utredningens utgångspunkter

Inom Sverige förefaller det finnas ett glapp i begrepp och definitioner mellan övergripande nivå och den vardag som branschens aktörer och användare möter. Detta nödvändiggör att begrepp och definitioner som rör informationssäkerhet på övergripande nivå måste konkretiseras ytterligare för att kunna tjänstgöra som verktyg i den praktiska vardagen och för att lättare kunna genomföra EU-bestämmelser inom ett antal områden.

Branschens möjlighet att formulera heltäckande krav och definitioner som uppfattas som tvingande är begränsat. Det är sannolikt endast statsmakterna som har denna möjlighet. Det är dock av stor vikt att det finna sådana begrepp och definitioner som kan binda samman ovanifrånperspektivet med underifrånperspektivet. Om en tydlighet på detta område kan uppnås blir det också lättare att i det kommande arbetet förankra förslag från utredningen.

Mot denna bakgrund har frågan om definitioner blivit en synnerligen viktig fråga för det fortsatta utredningsarbetet.

Utredningen kommer i betänkandet utgå från SIS definition av begreppet informationssäkerhet. Detta innebär att utredningen definierar informationssäkerhet som säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spårbarhet och oavvislighet. Begreppet innefattar såväl IT-säkerhet som säkerhet i administrativa rutiner.

Begreppet informationssäkerhet innefattar såväl det område som traditionellt benämnts datasäkerhet, som övriga begrepp som har anknytning till hur information skall kunna hanteras på ett säkert sätt i skilda slag av verksamheter. Utgångspunkten är att viss information kan vara kritisk i något avseende – genom att verksamheten och dess mål kan komma att äventyras om information skulle komma till obehörigs kännedom, modifieras, förstöras eller på annat sätt göras otillgänglig. Likaså kan verksamheten och dess mål äventyras om inte adekvat utbildning återfinns i, eller rätt förberedelser har genomförts inom organisationen.

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

1.2 Utvecklingstendenser

IT-utvecklingen påverkar i stort sett hela samhället på alla nivåer. Oavsett vilket mått som används för att beskriva utvecklingen – t.ex. total överföringskapacitet, antal fiberkablar, antal Internetanvändare, antal kommunikationsvägar mellan olika platser, eller antal kommunikationssatelliter –handlar det om en mångdubbling sedan början av 1990-talet.

Den tekniska komplexiteten ökar ständigt. IT-systemen blir allt kraftfullare med större minneskapacitet och snabbare processorer, vilka därmed också möjliggör utveckling och användande av program som kan utföra nya och mer komplicerade funktioner. I många fall har möjligheten att ersätta IT-system med manuella rutiner försvunnit. Det innebär att många organisationer är helt beroende av kontakt eller kommunikation med andra IT-system för sin

dagliga verksamhet, för t.ex. styr- och reglerfunktioner, ekonomiska och administrativa program m.m. Samtidigt fortsätter trenden mot integration av systemen i olika verksamheter, olika funktioner och hos olika aktörer. Leverantörer och beställare knyts ihop med distributören i en kedja som bygger på användningen av IT-system. IT-system utgör också en viktig del i styrning och kontroll av andra infrastrukturer som telekommunikation och för distribution av elkraft. När myndigheter, företag, organisationer och privatpersoner är sammankopplade via t.ex. Internet eller intranät, kan det innebära att det skapas möjligheter att nå information för andra än de som har behörighet. Det ökar också risken för manipulation, såsom att informationen raderas eller ändras. Spridningen av skadlig kod, t.ex. datavirus, kan gå oerhört fort och få en avsevärd omfattning. Andra typer av störningar kan också snabbt fortplanta sig i nätet.

Utvecklingen mot ökad sårbarhet motverkas dock av att säkerhetsmedvetenheten hos både leverantörer och kunder ökar. Producenter av program har också uppmärksammat säkerhetsfrågorna och satsar på att skapa säkrare produkter. Det finns också ett omfattande internationellt arbete kring standarder och andra stöd för att utveckla och utvärdera säkerheten.

Datorspridning är en central faktor i utvecklingen. Datorer och inbyggda system fortsätter att spridas i alla typer av miljöer och maskiner. Detta i kombination med sammankopplingen av system gör att beroendet av tekniken ökar samtidigt som förhållandena blir mer svåröverskådliga

Organisatoriska frågor påverkar också utvecklingen inom informationssäkerhetsområdet. En aktuell diskussion är frågan om att lägga ut IT-system på driftentreprenad (outsourcing). Det innebär att det dagliga ansvaret för driften av många system flyttas ut från företagen till en extern part. Det kan innebära en professionalisering och effektivisering av informationssäkerhetsarbetet samtidigt som möjligheterna till kontroll och inflytande förändras. Vissa lagar och regler ställer också krav på informationssäkerhetsarbetet.

I ett land som Sverige, med en tydlig politisk ambition att IT skall utgöra en strategiskt viktig komponent i samhället, finns det höga förväntningar på att tekniken skall fungera tillfredsställande och med förutsägbarhet. Utvecklingen inom säkerhetsområdet kan påverka förtroendet för den nya tekniken och dem som använder den.

Ökat beroende av IT samt svårigheterna att utveckla säkerheten i takt med hotutvecklingen gör det IT-relaterade hotet allt mer påtagligt. Förenklad inhämtning, bearbetning och lagring av information samt standardiserade produkter har successivt skapat möjligheter för en typ av aktör som tidigare inte hade kapacitet att på ett reellt sätt störa samhället (asymmetriskt hot[2]). Det är dock viktigt att i en hotbildsbeskrivning hålla isär olika aktörers möjligheter att genomföra angrepp och deras eventuella motiv och intentioner. De tekniska och strukturella möjligheterna visar på en potentiell hotbild men utgör i sig ingen förutsägelse.

Sverige har under lång tid legat långt framme när det gäller olika åtgärder för att öka robustheten inom olika samhällssektorer. El- och telekommunikation har varit prioriterade områden. Sedan dessa marknader avreglerades har statliga medel avsatts för investeringar i olika infrastrukturella åtgärder. Huvudsyftet har under tidigare år varit att förebygga skador som skulle kunna uppstå i samband med ett väpnat angrepp. Under de senaste åren har åtgärderna mer inriktats mot att även kunna motstå svåra påfrestningar. Det har dock inte gjorts någon uppföljning som gör det möjligt att bedöma vilka effekter åtgärderna haft.

1.3 Den informationsrelaterade hotbilden

Regeringen beskrev i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158) relationen mellan sårbarhet, hot och risk. Regeringen anser att de risker som finns i samhället bygger på ett samband mellan flera olika parametrar. En parameter är samhällets sårbarhet, en annan möjliga hot. Detta kan ligga till grund för en värdering av sannolikheten för att en allvarlig situation skall inträffa, samt de möjliga konsekvenserna. Utredningen har i betänkandet tagit detta resonemang som utgångspunkt.

Regeringen beskrev också i den ovan nämnda propositionen sin syn på informationssäkerhetshot och anförde där följande:

[2] Asymmetriska hot är benämningen på hot som har sin grund i att även en tekniskt eller materiellt svagare aktör kan anpassa och utnyttja sitt agerande för att utnyttja motpartens resursmässigt, politiskt eller psykologiskt svagare sidor. I USA kategoriseras exempelvis asymmetriska hot till nukleära, kemiska, biologiska, informationsoperationer, alternativa operationskoncept samt terrorism..

”Erfarenheter från det säkerhetsarbete som bedrivits av myndigheter och företag visar att den största sårbarheten kan härröras till oavsiktliga tekniska fel, bristande planering m.m. som leder till driftstörningar. Vidare är sårbarheten avseende avsiktliga hot stor då det gäller egna anställda (s.k. insiders). Möjligheterna för någon inom en organisation att obehörigt föra med sig hemligheter ut eller att förbereda ett system för en attack utifrån är relativt stora. Förmågan att möta allvarliga hot är beroende av ett grundläggande säkerhetsarbete som i första hand skyddar mot de vardagliga säkerhetsproblemen. De allvarliga kända angrepp som Sverige hittills utsatts för har riktats mot specifika verksamheter och organisationer. I likhet med många andra länder har Sverige under senare år blivit utsatt för stundtals mycket omfattande datavirusspridning. Dessa angrepp har dock varit mer slumpartade än riktade. Vid angreppen har de uppkomna skadorna i form av avbrott och stillestånd blivit relativt begränsade vad gäller samhällsviktiga infrastrukturer, men har icke desto mindre medfört stora kostnader för de drabbade. Det har även förekommit riktade angrepp, i form av hot, överbelastnings- och tillgänglighetsattacker av olika slag riktade mot personer, organisationer och företag som ådragit sig andra individers eller gruppers missnöje.

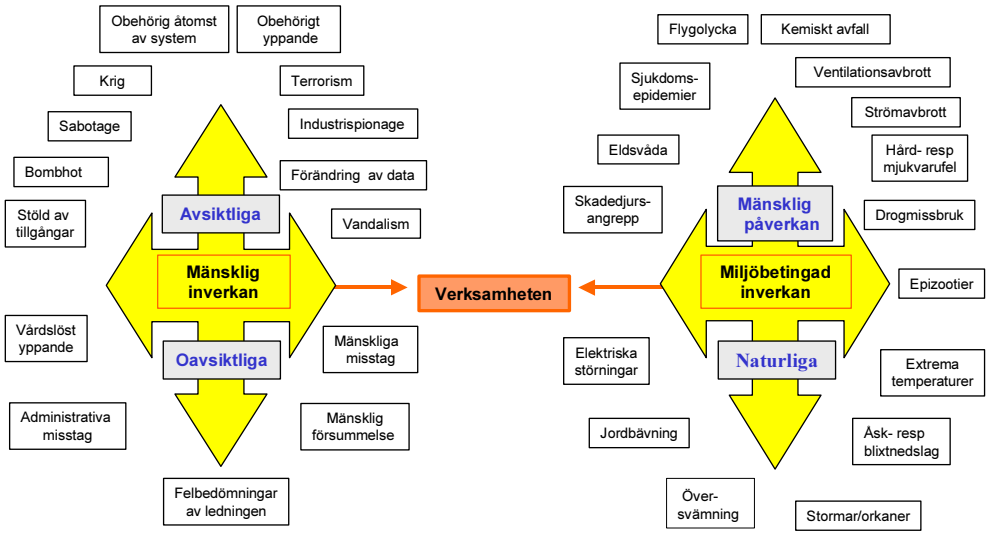
Kända angrepp från utländska aktörer mot Sverige och svenska intressen har hittills varit relativt begränsade och medfört begränsad skada. De mer omfattande angrepp som ändå förekommit, har utförts av nätverk av angripare och har bemötts genom samarbete inom de angripna strukturerna.

Ett ständigt närvarande hot är det som kommer från underrättelseverksamhet riktad mot Sverige och svenska intressen. Den nya informationstekniken har inneburit att ytterligare möjligheter att tillskansa sig information genom både öppen och hemlig (illegal) verksamhet har skapats.”

Utredningen anser att ovanstående beskrivning av hotbilden alltjämt är giltig, och att det är av stor vikt att utgå från en sådan helhetssyn när en bedömning sker av hur informationssäkerhet skall byggas inom olika verksamhetsområden.

Utredningen konstaterar att det finns anledning att inom några områden utveckla beskrivningen av den informationsrelaterade hotbilden. Nedanstående bild utgör därvid en utgångspunkt. Bilden illustrerar att den informationsrelaterade hotbilden omfattar både s.k. ’mänsklig inverkan’ (avsiktlig som oavsiktlig) liksom ’miljöbetingad inverkan’ (naturlig såväl som genom mänsklig påverkan).

Hot och sårbarheter



1.3.1 Ökad komplexitet kräver samarbete

Då många system är komplexa och i många fall hopkopplade kan det ibland vara svårt att avgöra var eller hur ett fel eller en störning har uppstått. I den mån det rör sig om en avsiktlig attack finns det stora möjligheter att dölja attackens ursprung. Detta medför att det är svårt att vara oberoende i sitt informationssäkerhetsarbete. Den enskilda organisationen är beroende av sina leverantörer (t.ex. program och kommunikationer) och samarbetspartner (t.ex. genom gemensamma nät eller andra typer av sammankopplingar). För vissa branscher kan dessa beroenden bilda komplexa mönster. I en tilltagande internationalisering innebär det att dessa förhållanden spänner över flera länder. Det påverkar i hög grad möjligheterna till ett samlat informationssäkerhetsarbete. På ett övergripande plan är det nödvändigt att samverka med aktörer i andra länder för att gemensamt söka uppnå en tillfredsställande säkerhetsnivå. Samarbete

med andra länder är viktigt också på den operativa nivån, t.ex. när det gäller att spåra IT-brottslingar.

1.3.2 Olyckor och misstag

Den informationsrelaterade hotbilden har under senare år fått stor uppmärksamhet i den offentliga debatten. Det som främst diskuteras är de nya sårbarheterna som uppstått i och med informationsteknikens införande på i huvudsak el- och telemarknaderna. Härvidlag har informationstekniska hot (IT-hot), och hotet från s.k. informationsoperationer (IO) övergripande diskuterats och debatterats. Det är dock viktigt att konstatera att IT-hoten endast är en del av de informationssäkerhetsrelaterade hoten. Händelser som åsknedslag, avgrävda ledningar för el och tele, bristande rutiner och handhavandefel är de absolut vanligaste orsakerna till problem.

Hot som beror på olyckor och misstag är svåra att förutsäga, och det är också svårt att bedöma deras konsekvenser. I det följande ges några exempel på hot som beror på olyckor och misstag.

- Ovana användare eller andra kan oavsiktligt skada IT-system. Även om det inte är deras avsikt kan följderna bli att det uppstår störningar eller skador i IT-system. Det kan röra sig om röjande av information som kan användas för att störa systemet, administrativa misstag som att inte avsluta användarkonton eller begränsa rättigheter när de inte längre behövs för personal eller konsulter, eller förlust av information genom att den raderas av misstag.
- Användare och systemadministratör kan också skada ett system eller störa tillgängligheten p.g.a. otillräcklig kompetens eller utbildning. Dessa personer har kanske inte som motiv att störa ett system, men deras arbetsuppgifter kan vara av den karaktären att de, om de inte sköts korrekt, ger upphov till skador och störningar.
- Nyinstallation och uppgraderingar av infrastruktur för pro-gram och datorutrustning är ofta komplicerade processer. Sådana infrastrukturer och deras förhållande till program m.m. kan vara komplexa och medföra risker för t.ex. störningar i tillgänglighet eller förlust av data.

- Oavsiktliga fel i design, införande och testning av IT-system kan leda till att en tjänst inte fungerar eller att data försvinner. En missbedömning av kapacitetsbehovet kan t.ex. leda till överbelastning och därigenom störningar i tillgänglighet.
- Felaktig information, kanske till följd av bristande rutiner, kan ge felaktiga resultat eller undergräva förtroendet för ett system.
- Program eller datorutrustning som inte fungerar kan orsaka förlust av data eller störningar i en tjänst.
- Olyckshändelser som brand, översvämning m.m. kan förstöra utrustning och information så att en tjänst inte går att upprätthålla.

1.3.3 Program, datorutrustning och komponenter

De områden som den snabba teknikutvecklingen har påverkat vad gäller informationssäkerhetsarbetet är bl.a. bredbandsutvecklingen, öppen källkod, trådlösa lokala nät (så kallade trådlösa LAN) och icke-hierarkiska nät (peer-to-peer).

Bredbandsutvecklingen leder till att fler klienter ständigt ligger uppkopplade med hög kapacitet, vilket medför ökad risk för att dessa klienter kan komma att bli agenter för exempelvis distribuerade tillgänglighetsattacker. Utöver att slutanvändarens utrustning är exponerad under lång tid för angripare kan dessa dessutom dra fördel av den höga anslutningskapaciteten.

En trend i arbetet för att uppnå säkrare system är att flera olika leverantörer av program används för att på så sätt sprida riskerna inom exempelvis statsförvaltningen. Detta är ett av skälen till att det inom många administrationer världen över diskuteras om program baserade på öppen källkod skall ersätta proprietära program. Andra skäl kan vara ekonomi och politik. Med öppen källkod ges också möjlighet att kontrollera och modifiera de program som användaren installerar. Denna möjlighet gör att säkerheten i system kan ökas genom att koden kan inspekteras och onödiga funktioner tas bort. I debatten har framförts att en baksida med öppen källkod kan vara att dagens program är mycket komplexa, samt att kodanalys är en svår och dyr verksamhet vilket kan medföra en risk att ingen klarar av att utföra kontrollen fullt ut. Detta kan i sin tur in-

nebära att öppen källkod kan inge en falsk trygghetskänsla. Öppen källkod kan också göra det lättare för en eventuell angripare att både identifiera och utnyttja svagheter. Detta skall dock ställas i relation till proprietär programvara där användaren har mycket begränsad insyn i innehåll, liksom omfattning och kvalitet i leverantörens interna kodanalys.

Trådlösa LAN innebär trådlös uppkoppling inom ett begränsat geografiskt område. Då möjligheterna att fysiskt förhindra obehöriga att använda nätet är svåra, ökar riskerna för att nätet används av andra än vad som var tänkt.

De ökande möjligheterna till informationsspridning genom t.ex. högre kapacitet, peer-to-peer-nätverk m.m. kan leda till en större spridning av filer infekterade av skadlig kod.

Utvecklingstendenserna för Internet är att det expanderar vad gäller antalet användare, trafikmängd, tillämpningar, antalet IP-adresserbara enheter inklusive mobila terminaler (t.ex. mobiltelefoner). I takt med detta ökar även såväl omfattningen som komplexiteten i Internets infrastruktur: fler routrar, fler domännamnsservrar[3], fler knutpunkter, mer kabel, fler radiosändare m.m.

För domännamnssystemet (DNS) är en trolig utveckling att allt fler funktioner och tjänster kommer att hanteras, exempelvis utökade säkerhetsfunktioner (DNSSEC), nummersättning av IP-telefoni (ENUM), lagring av digitala certifikat etc., vilket ytterligare kommer att öka domännamnsystemets betydelse.

Rotservrarna är en viktig del i DNS, de måste vara stabila och ha gott skydd. Det är också angeläget med internationalisering av arbetet med DNS. Det är t.ex. angeläget att säkerställa robust drift av den nationella toppdomänen och andra viktiga funktioner för Internet i Sverige, med hög tillgänglighet till DNS och ett betryggande system för hur informationen i DNS uppdateras. Bland hoten mot DNS och andra delar av Internet märks bl.a. distribuerade överbelastningsattacker.

[3] Domännamnsystemet i Internet (Domain Name System, DNS) översätter mellan domännamn och IP-adresser, t.ex. www.google.com och adressen 66.102.11.99.

Samtidigt ligger många viktiga informationssäkerhetsfrågor för Internet i utkanten av nätet, eller på andra nivåer. Det finns även risker förknippade med att samma produkter och program används i både nätutrustningen, domännamnsservrar, routrar och i de anslutna datorerna. En säkerhetsbrist i en produkt som är väldigt spridd kan medföra att försök att utnyttja den kan få stora och snabba konsekvenser.

En utvecklingstrend som kan komma att påverka det framtida arbetet med informationssäkerhet är integrering av program och datorutrustning. Ett exempel är att integrera program och datorutrustning för att enskilda persondatorer skall kunna fungera på ett säkrare sätt vid exempelvis elektronisk handel. Detta kan i vissa fall vara en positiv utveckling då det bl.a. möjliggör autentisering, identifikation, kryptering och kontroll av installerade pro-gram. Det är dock en utveckling som bygger på centralstyrning av licensanvändning m.m. Centralstyrningen innebär att om systemet utvecklas på fel sätt kan det missbrukas för att kontrollera enskilda persondatorer som är anslutna till t.ex. Internet.

1.3.4 Insider-problematiken

De största källorna till informationssäkerhetsproblem är ofta anställda (konsulter m.m.) i den egna organisationen, s.k. insiders. De kan ha stora möjligheter att störa system. Programutvecklare, systemadministratörer, driftpersonal och andra kan ha kunskap om konstruktionen och brister i program och system som kan utnyttjas för den som vill angripa systemet. Insiderna kan också förmås att delge den informationen till andra som kan angripa systemen utifrån. Personerna kan också ha omfattande rättigheter i systemet som ger dem tillgång till information och möjligheter att påverka systemen. Med dagens lagringsmedier är det också möjligt att stjäla stora mängder information och föra ut den obemärkt på cd-skivor, minneskort etc.

Insiderproblemet är svårt att komma åt. I en bred bemärkelse är det ofta en personalfråga. Det gäller från rekrytering till avslutande av anställningen, ibland även efter det – och på motsvarande sätt för t.ex. konsulter. Det är ofta personer som känner sig illa behandlade som vänder sig emot organisation. Andra åtgärder är att ha rutiner och regler, som personalen följer, som stödjer det tekniska säker-

hetsarbetet. Andra möjligheter är att genom rättigheter och loggar begränsa och följa upp hur systemen används.

När det gäller personer som deltar i verksamhet som har betydelse för rikets säkerhet eller för skyddet mot terrorism finns bestämmelser i säkerhetsskyddslagen om säkerhetsprövning för att klarlägga om personen kan antas vara lojal och pålitlig ur säkerhetssynpunkt.

1.3.5 Underleverantörer

Den snabba teknikutvecklingen har medfört att många IT-företag idag av kostnadsskäl eller för att kunna följa med i den snabba utvecklingen förlitar sig på underleverantörer, inklusive driftentreprenad (outsourcing). Det kan finnas fördelar med användningen av underleverantörer även ur ett säkerhetsperspektiv t.ex. genom större tillgång till säkerhetsexpertis eller effektivare och enhetligare säkerhetsarbete. Samtidigt kan det ökande användandet av underleverantörer påverka arbetet med informationssäkerhet negativt, då det är svårt att kontrollera hela utvecklingsprocessen. Det kan exempelvis vara svårt att få svar på vem som har tillverkat koden till programmens alla delar. Det kan vara en underleverantörs underleverantör som tillverkat koden, och det kan vara svårt att överblicka om någon eller några av de inblandade i utvecklingskedjan kan ha haft dolda motiv. Detta problem är intimt kopplat till den ökade komplexiteten hos moderna program som beskrevs tidigare.

Nyttjandet av underleverantörer och övergången till projektorganisationer har ytterliggare ökat den redan stora personalrörligheten inom IT-branschen. Här finns ett potentiellt hot från kvalificerade insiders som kan ha olika motiv. Det kan vara allt från konsulter som känner sig förorättade till systematiskt planerade attacker. Attacker som är systematiskt planerade kan börja med att en programmerare hos en underleverantör konstruerar en bakdörr i en modul till ett stort datasystem. Därefter söker personen anställning inom en organisation som använder det aktuella systemet och kan då nyttja sin inplacerade bakdörr. Problemet är inte nytt men möjligheterna till kontroll av processen från programmering till installation av program är idag mycket mer begränsade än de var tidigare.

1.3.6 IT-relaterad brottslighet

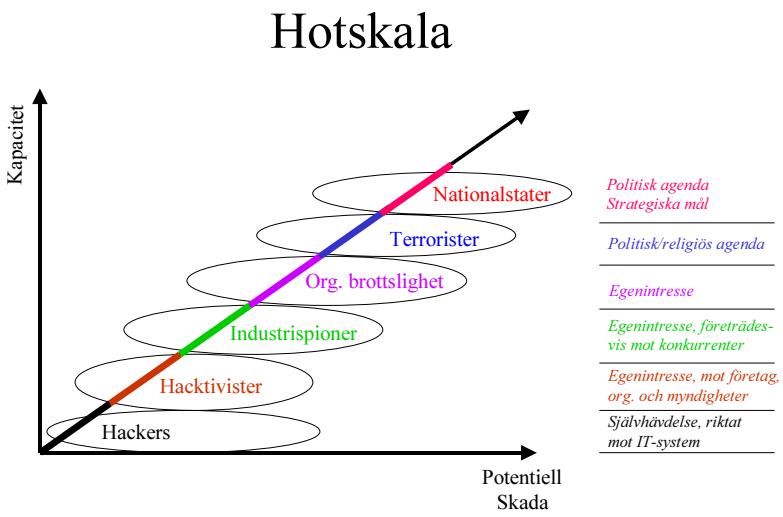
Ett växande problem idag är IT-relaterad brottslighet. Förhållandet mellan IT-relaterad brottslighet och informationssäkerhet är inte enkel. Brottslingar kan använda tekniken för att underlätta sin verksamhet och att begå brott. Olika säkerhetsfunktioner, som t.ex. kryptering av information, kan användas för att dölja brottslig verksamhet. Teknikutvecklingen i sig ger också upphov till nya möjligheter att begå brott. Å andra sidan öppnar teknikutvecklingen också för nya möjligheter att utreda brott, och ett ökat informationssäkerhetsarbete kan i många fall förhindra eller försvåra för någon att begå brott.

1.3.7 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 kunna innebära ett hot mot rikets säkerhet. Dessa hot utgör självfallet också ett hot mot många andra verksamhetsområden. Var gränsen går mellan mer allmänna hot och hot mot rikets säkerhet är inte absolut.

Aktörerna är inte heller alltid enhetliga eller lätta att definiera. En hackare kan gå från att hacka för egen räkning till att arbeta inom ramen för organiserad brottslighet eller för någon annan aktör.

Bilden nedan åskådliggör relationen mellan hot och aktörer och vilken skada de kan tänkas åstadkomma. Stater kan antas ha övergripande politiska och långsiktiga strategiska mål. Terrorister kan antas ha någon form av politiska eller religiösa mål medan den organiserade brottsligheten i huvudsak kan förväntas ha egenintresset som drivkraft. Även när det gäller olika typer av industrispionage kan det huvudsakliga intresset vara någon form av egenintresse men då kanske främst riktat mot konkurrenter. När det sedan gäller vad som här benämns hacktivister, t.ex. olika typer av politiska grupperingar, kan även dessa antas styras av intresset att driva de egna frågorna. Den sista gruppen enligt denna indelning är då den enskilda hackaren.



Tidsförhållandena är också en viktig faktor. Vissa attacker kan gå väldigt fort att genomföra men vara svåra att använda för att nå precisa mål. Datavirus kan få en snabb, men okontrollerad spridning. Att kartlägga och undersöka system för att få t.ex. ökad precision eller effekt i attacker kan vara kostsamt och ta lång tid. Det ökar också risken för att bli upptäckt. De olika aktörerna har olika förutsättningar och intressen som påverkar inom vilken tidsram man agerar.

Det huvudsakliga problemet är att urskilja vilken aktör som är aktiv; är det en hackare eller en stat som agerar, eller något däremellan?

Datornätverksoperationer

Flera stater satsar idag stora resurser på underrättelseinhämtning och desinformation via något som skulle kunna kallas det globala nätet. Det globala nätet kan ses som helheten av kommunikation, oavsett om den går via Internet, i radionät eller telenät, och oberoende av vilket medium som används (kablar, länkar, radiovågor etc.). För kvalificerade aktörer kommer det att vara möjligt att hämta och sprida information via det globala nätet. Det kommer

också att finnas möjligheter att påverka utrustning med hjälp av nätet för att stödja de egna insatserna. Även om Sverige inte direkt är inblandat i en konflikt finns det risk att nät och utrusning placerad i Sverige eller ägd av svenska intressen utnyttjas för sådana operationer i något tredje land. Ett ofta använt samlingsbegrepp för denna typ av verksamhet är s.k. datornätverksoperationer (DNO).

Datornätverksoperationer kan delas in i tre huvudgrupper; datornätverksinhämtning, datornätverksattacker och datornätverksförsvar[4].

Datornätverksinhämtning innebär att inhämta information via det globala nätet, främst Internet, men även i lokala nätverk. Detta kan exempelvis göras genom att skapa ett program som gör det möjligt att ta sig in i de system som lagrar informationen.

Med datornätverksattacker menas att en aktör utnyttjar det globala nätet för att störa eller slå ut delar av en informationsinfrastruktur. Datornätverksförsvar innebär att skydda sig mot inhämtning och attack.

I många länder omgärdas det som rör offensiv, och i vissa fall även defensiv, IT-förmåga med mycket hög sekretess. Satsningar på denna typ av verksamhet är därför ofta svåra att identifiera. Till viss del kan de följas genom att granska de satsningar som sker på underrättelsetjänst och signalspaning.

Målet med datornätverksinhämtning är att inhämta underrättelser från informations- och tjänsteflödet i det globala nätet. Metoderna kan variera, från traditionell underrättelseverksamhet till kartläggning av de tekniska aspekterna av det globala nätet inför en datornätverksattack. De aktörer som syns och diskuteras i den offentliga debatten är de illegala och legala aktörerna i form av hackare och andra typer av IT-brottslingar samt öppna statliga och andra organ som försöker bekämpa denna verksamhet. De medel som de illegala aktörerna har till sitt förfogande är ett antal kända metoder och verktyg: datavirus, trojaner, DNS-attacker, tillgänglighetsattacker, fjärrstyrning m.m.[5] Samhället försöker möta denna verksamhet

[4] Inom Försvarsmakten kallas datornätverksförsvar för IT-försvar.
[5] DNS=domännamnservrar. Genom att föra in felaktig information kan användare styras om till en ”falsk” adress eller server, vilket i sin tur kan utnyttjas för bedrägerier eller desinformation. DoS=Denial of Service. Förhindrar användning av ett system, ett nät eller tjänst

med olika metoder t.ex. med s.k. Computer Emergency Response Teams (CERT-funktioner) och andra säkerhetshöjande åtgärder, så som nätverksövervakning och olika typer av antivirusprogram etc.

Vidare kan konstateras att det finns ett antal aktörer, främst nationalstater, som utvecklar, har tillgång till och använder metoder som det finns mycket begränsad allmän kännedom om.

Fysiska hot

Ett annat allvarligt problem är olika former av fysiska hot och vapen. Beroende på storlek av vapnet, avstånd till målet och målets skyddsnivå kan t.ex. ett HPM-vapen förorsaka permanent fysisk skada, permanent funktionsfel, temporärt avbrott, prestandanedsättning eller temporär störning. Hotet från HPM-vapen är en realitet redan idag och nya metoder är under utveckling. Det finns dock ännu inga kända fall av HPM-attacker.

Växelverkanseffekter genom datavirus och datamaskar

Intrikata växelverkanseffekter (s.k. epidemiska effekter) mellan enheter inkopplade på publika nät av Internettyp kan orsaka allvarliga och ibland svårbemästrade störningar i trafiken av epidemisk natur. Exempel på detta är spridningen av datavirus och datamaskar. Vid flera tillfällen har t.ex. datamaskar lett till att organisationers Internetanslutna funktioner blockeras helt eller störs allvarligt (t.ex. I Love You-, Melissa- och SobigF-virusen, maskarna Slammer, Blaster etc).

Sårbarheten uppstår bl.a. som en effekt av att många anslutna datorer har likartad konfiguration och därmed delar samma svagheter ,med möjlighet till automatiserade intrång. Den förvärras även av det faktum att kommunikationsprotokollen har svagheter eller felaktigheter som kan ge upphov till, eller utnyttjas till att skapa, olika typer av svårkontrollerade effekter. Genom att nätets kapacitet också kan påverkas, försvårar detta även samordnande och avhjälpande insatser, t.ex. genom att dataviruset försöker blockera en av leverantörens uppdateringsservrar.

(t.ex. överbelastning). Fjärrstyrning=av dator från en annan dator, t.ex. BackOffice, Sub-7 ocb Netbus.

Dessa spridningseffekter beror på vilka programversioner och konfigurationer som används. I många fall får man ett globalt förlopp i andra fall begränsat till t.ex. olika språkversioner av ett operativsystem.

2 Informationssäkerhet i Sverige

Detta kapitel är en översiktlig beskrivning av informationssäkerhetsarbetet i Sverige, så som det ser ut i dag. Kapitlet behandlar den offentliga sektorn, där utvecklingen av informationssäkerhetsarbetet beskrivs, och verksamhet och inriktning på nationell nivå samt hos vissa berörda myndigheter. Dessutom ges en kort beskrivning av ett antal aktörer på den privata sidan, dessa organisationers övergripande perspektiv på informationssäkerhetsfrågor, och behovet av samverkan mellan offentlig och privat verksamhet inom området informationssäkerhet.

2.1 Informationssäkerhetsarbetet i offentlig sektor

2.1.1 Utvecklingen av det svenska informationssäkerhetsarbetet

Sverige har genom det IT-politiska beslut som fattades år 2000 formulerat ett IT-politiskt mål att Sverige skall vara det första land som blir ett informationssamhälle för alla. Detta mål täcker hela det IT-politiska området. De områden som prioriteras är tillit, tillgänglighet och kompetens. Tillit och tillgänglighet handlar till stor del om teknik och elektroniska kommunikationsnät, medan det tredje området kompetens är av en annan karaktär. Genom dessa tre områden kan och avser regeringen att påverka användningen av IT. I det IT-politiska målet rörande tillit ryms frågor som rör säkerhet och personlig integritet. Regeringens inriktning avseende tillit är att regler och system på IT-området bör vara sådana att de skapar förtroende genom att vara säkra, förutsebara och teknikneutrala. De bör också kunna skydda individens integritet samt vara internationellt accepterade. Ansvaret för informationssäkerheten ligger

hos de myndigheter, företag och organisationer som har det normala verksamhetsansvaret. En annan viktig aspekt av det IT-politiska målet är tillgänglighet. Detta innefattar bedömningen att hushåll och företag i alla delar av landet inom de närmaste åren bör få tillgång till IT-infrastruktur med hög överföringskapacitet och liten fördröjning, men också med hög tillgänglighet och robusthet hos nät och nätresurser.

I maj 2001 lämnade Sårbarhets- och säkerhetsutredningen sitt betänkande Säkerhet i en ny tid (SOU 2001:41). I detta betänkande presenterade utredningen bl.a. ett förslag till övergripande strategi för samhällets hantering av IT-säkerhet, samt förslag till inrättande av ett antal nya funktioner. Inom IT-säkerhetsområdet kan Sårbarhets- och säkerhetsutredningens förslag rörande de nya funktionerna sammanfattas enligt nedan:

- Ett tvärsektoriellt samordningsorgan för IT-säkerhet och skydd mot informationsoperationer inrättas i Regeringskansliet.
- Att den av utredningen föreslagna planeringsmyndigheten (den senare etablerade Krisberedskapsmyndigheten – utredningens anmärkning) får ett sammanhållande ansvar för samhällets IT-säkerhet (i instruktionen sedan omformulerat till informationssäkerhet – utredningens anmärkning).
- En funktion för teknikkompetens inom IT-säkerhet, vilken inrättas i s.k. FRA-miljö som en egen myndighet med Försvarets radioanstalt som chefsmyndighet
- En funktion för IT-incidenthantering, vilken inrättas i högskolemiljö som en egen myndighet med Post- och telestyrelsen som chefsmyndighet.
- Att den funktion som inrättas för omvärldsanalys, vilken inrättas som en del i planeringsmyndigheten, även har kapacitet att bedriva omvärldsanalys inom områdena IT-säkerhet och informationsoperationer.
- Att Försvarets materielverk bör ges i uppgift att bygga upp ett svenskt system för evaluering och certifiering av IT-säkerhet i produkter och system.

Bakgrunden till Sårbarhets- och säkerhetsutredningens förslag var utredningens konstaterande att Sverige, till skillnad från många andra länder, saknade ett sammanhållet system för att hantera allvarliga IT-hot. Verksamheten konstaterades vara uppsplittrad på

många organ i samhället och ansvarfördelningen mellan dessa bedömdes i många fall också vara oklar. Denna slutsats gällde enligt Sårbarhets- och säkerhetsutredningen också för statens satsningar inom IT-säkerhetsområdet. Sårbarhets- och säkerhetsutredningen konstaterade att staten måste ta ett ansvar inom informationssäkerhetsområdet, samtidigt som den verksamhetsansvariges och systemägarnas ansvar för att säkra de egna systemen mot IT-intrång och andra typer av IT-hot också betonades. Statens roll borde därför enligt Sårbarhets- och säkerhetsutredningen vara att stödja detta arbete och att svara för funktioner som samhället i övrigt har svårt att organisera. Ambitionsnivån inom många områden ansågs behöva höjas och ansvarsförhållandena tydliggöras.

Sårbarhets- och säkerhetsutredningen framhävde även behovet av ett antal författningsförändringar för att stödja de förslag som utredningen redovisade. Författningsförändringar bedömdes av Sårbarhets- och säkerhetsutredningen behövas för att tillgodose följande behov:

- En hög sekretess behöver tillämpas inom IT-teknikkompetensfunktionen och IT-incidenthanteringsfunktionen, vilket kan kräva lagändringar.
- En aktiv IT-kontroll med sanktionerade intrångsförsök i viktiga system måste kunna bedrivas. De lagtekniska förutsättningarna för detta behöver belysas.
- Regler om obligatorisk incidentrapportering bör införas inom statsförvaltningen. Denna skyldighet för myndigheterna bör författningsregleras.

(För vidare behandling av författningsmässiga frågeställningar, se kapitel 3 och 6.)

Efter att Sårbarhets- och säkerhetsutredningen lagt fram sitt betänkande, redovisade regeringen i två följande propositioner Fortsatt förnyelse av totalförsvaret (2001/02:10) och Samhällets säkerhet och beredskap (2001/02:158), att regeringen avsåg att inrätta fyra verksamhetsområden i syfte att förbättra informationssäkerheten. De fyra verksamhetsområdena var omvärldsanalys, IT-incidenthantering, teknikkompetens, samt ett system för evaluering och certifiering. För att snabbt kunna stärka informationssäkerheten föreslog regeringen att de nya uppgifterna borde fördelas

på de myndigheter som redan sedan tidigare bedrev närliggande verksamhet. Regeringen betonade dock att en utvärdering avsågs genomföras efter två år, då andra organisatoriska lösningar inom informationssäkerhetsområdet skulle kunna komma att bedömas vara lämpliga. I de nämnda propositionerna föreslog regeringen följande ansvarsfördelning:

- Krisberedskapsmyndigheten bör ges ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. I detta bör ingå att följa upp och utvärdera informationssäkerheten i samhället och att årligen lämna en samlad bedömning till regeringen. Krisberedskapsmyndigheten bör också tillse att det utvecklas ett samarbete mellan offentlig sektor och näringsliv inom informationssäkerhetsområdet.
- Post- och telestyrelsen bör få i uppgift att ansvara för hantering av uppgifter om IT-incidenter.
- Försvarets radioanstalt bör ges ansvar att tillhandahålla teknikkompetens inom informationssäkerhetsområdet.
- Försvarets materielverk bör få i uppgift att bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter.

Regeringen meddelade även i propositionen 2001/02:158 att en översyn av författningar som berör informationssäkerhetsområdet bör genomföras.

Regeringen slog i propositionen 2001/02:158 också fast principen att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande. Statens roll är därmed att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den egna systemägaren.

I arbetet med utvecklingen av samhällets förmåga att hantera sårbarhets- och säkerhetsfrågor ur ett bredare perspektiv, betonades tidigt betydelsen av ansvarsprincipen som grund. Ansvarsprincipen innebär att var och en inom sitt område skall ansvara för förebyggande arbete och hantering av hot och risker i hela skalan från fred till krig. Parallellt med denna princip betonades också behovet av en utvecklad struktur för samordning och gemensam hantering av tvärsektoriella hot. I samband med Sårbarhets- och säkerhetsutredningens arbete utvecklades innehållet i ansvarsprincipen ytterligare.

I praktiken har ansvarsprincipen tolkats som att den myndighet eller det organ som har den i förhållande till krigsuppgiften mest näraliggande uppgiften, har tilldelats ansvaret. Detta innebär att myndigheten skall genomföra de beredskapsförberedelser som krävs för krigsuppgiften. Successivt har ansvarsprincipen även kommit att omfatta ett bredare perspektiv, då den även relateras till hela hotskalan och därmed även omfattar händelser som kategoriseras som svåra påfrestningar på samhället i fred.

Även i den strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system, som regeringen presenterade i propositionen 2001/02:158, är ansvarsprincipen, tillsammans med likhetsprincipen och närhetsprincipen utgångspunkten. Likhetsprincipen innebär att en verksamhets organisation och lokalisering så långt som möjligt skall överensstämma i fred, kris och krig. Närhetsprincipen innebär i sin tur att kriser skall hanteras på lägsta möjliga nivå i samhället. I strategin anges att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall kunna fungera tillfredsställande. Grunden är att myndigheter, organisationer, och företag som är systemägare har det primära ansvaret för informationssäkerhetsarbetet inom respektive ansvarsområde, och att staten kompletterar med åtgärder på vissa särskilda områden. I samband med att strategin presenterades redogjorde regeringen för en övergripande bedömning till grund för beslutet. För att kunna motstå IT-relaterade hot betonade regeringen att en bred kompetens krävs på alla verksamhetsnivåer i samhället. Att bygga upp en sådan kompetens på kort sikt är inte helt enkelt. Genom olika former av nätverk mellan organisationer och genom att successivt tillföra funktioner som saknas bedömde regeringen att säkerheten och skyddet ändå gradvis skulle kunna stärkas. Utifrån detta perspektiv kan regeringens beslut att inrätta de ovan nämnda fyra verksamhetsområdena, i syfte att förbättra informationssäkerheten, betraktas som en kompletterande förstärkningsåtgärd i relation till ansvarsprincipen. Samtidigt kan fördelningen av uppgifterna sägas ha utgått från ansvarsprincipen, då verksamheterna har fördelats till myndigheter med sedan tidigare närliggande uppgifter.

2.1.2 Informationssäkerhetsarbetet på nationell nivå – mål och ambitioner

I detta kapitel redogörs för informationssäkerhetsarbetet i Sverige på den nationella nivån. Beskrivningen baserar sig huvudsakligen på underlag från respektive departement. I arbetet med att få en övergripande bild av inriktningen av verksamheten på den nationella nivån, har utredningen varit i kontakt med samtliga sakdepartement. Underlag har inte erhållits från samtliga departement, och endast de som har beskrivit sin verksamhet finns därför med i presentationen nedan.

Utifrån det underlag utredningen fått del av, konstaterar utredningen att informationssäkerhetsfrågorna tycks vara olika väl förankrade inom de olika verksamhetsområdena. Utredningen avser därför i det fortsatta arbetet sträva efter att få en ytterligare kompletterad bild av informationssäkerhetsarbetet på den nationella nivån.

Justitiedepartementets verksamhetsområde.

Inom Justitiedepartementets område behandlas informationssäkerhetsfrågor utifrån främst tre perspektiv: a) lagstiftning som rör dataintrång och annan IT-brottslighet (straffrättsenheten), b) frågor som rör polisens möjligheter att utreda och beivra IT-relaterad brottslighet (polisenheten), c) frågor som rör skydd för den personliga integriteten (grundlagsenheten).

I praktiken går dessa frågor in i varandra och visar sig inte sällan vara sidor av samma mynt. Balansen mellan integritetsfrågor och polisens möjligheter att utreda IT-relaterad brottslighet är ett tydligt exempel på detta.

På grund av IT-brottslighetens gränsöverskridande och enhetsöverskridande karaktär, har Justitiedepartementet lagt den samordnande funktionen för internationellt IT-säkerhetssamarbete på EU-enheten. De internationella IT-säkerhetsfrågorna omfattar en rad initiativ, instrument och besluts- och förhandlingsprocesser som alla syftar till att skydda den snabbt växande informationstek-

nikens användning i samhället mot de hot som den IT-relaterade brottsligheten utsätter samhället, medborgarna, konsumenterna och näringslivet för.

Departementets hantering av IT-säkerhetsfrågorna präglas av den stora mängd frågor och instrument som ligger utanför Justitiedepartementets ansvarsområde men som indirekt berör departementet genom dessas kopplingar till IT-relaterad brottslighet. Närhelst IT-säkerhet diskuteras berörs Justitiedepartementets domän, eftersom den säkerhet som försöks upprätthållas till stor del rör sig om skydd mot olika former av intrång och angrepp, vilka nästan alltid är brottsliga.

Justitiedepartementets arbete med IT-säkerhetsfrågor syftar till att skapa förutsättningar för effektivt förebyggande av brott och en effektiv brottsbekämpning, samt ett starkt skydd för den enskildes rättigheter och integritet. Denna målsättning genomsyrar arbetet både på nationell och internationell nivå.

Inom Justitiedepartementets område är Säkerhetspolisen, Rikskriminalpolisen, Ekobrottsmyndigheten och Riksåklagaren viktiga aktörer. När det gäller myndigheter som lyder under Justitiedepartementet har dessa egna kontakter med andra myndigheter (t.ex. Krisberedskapsmyndigheten) som inte går via departementet. För polisens del är IT-brottsroteln på Rikskriminalpolisen en central kontaktpunkt.

Internationellt sker samverkan inom EU, Europarådet, OECD, G8, Interpol och Europol. Arbetet inom EU sker huvudsakligen inom den tredje pelaren men även inom den första pelaren. Inom den tredje pelarens verksamhet återfinns de polisiära och straffrättsliga frågorna. Idag pågår sammanlagt ett 50-tal processer inom EU som har någon bäring på IT-säkerhetsfrågorna. EU får betraktas som det viktigaste samverkansforumet. Inom Europol sker samverkan bl.a. kring barnpornografibrott på Internet. På myndighetsnivå försiggår nordiskt och även nordiskt-baltiskt samarbete.

Länderna på kontinenten delar vanligtvis upp ansvarsområden så att brottsbekämpningen faller på inrikesministeriets lott medan straffrätt och skyddet av den individuella integriteten ligger hos justitieministeriet. För svensk del samlas dessa ansvarsområden på olika enheter på Justitiedepartementet vilket ställer höga krav på

intern samordning, framför allt vad avser det internationella agerandet. Det är skälet till att det 2001 inrättades en samordningsfunktion vid enheten för EU- och internationella frågor (EU-enheten) med ansvar för internationella IT-säkerhetsfrågor. Möjligheten att förfina detta samordningsinstrument undersöks kontinuerligt.

Utrikesdepartementets verksamhetsområde

Europeiska rådets säkerhetsföreskrifter innehåller krav på att upprätta en nationell säkerhetsmyndighet. Motsvarande bestämmelser finns också vad gäller Sveriges åtaganden gentemot Nato och Europeiska rymdorganet (ESA). Regeringen har löst denna fråga genom att ange att enheten för säkerhet, sekretess och beredskap inom UD (UD-SSSB) skall upprätthålla funktionen som nationell säkerhetsmyndighet. Regeringen har vidare gett i särskilt uppdrag till Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Säkerhetspolisen, Riksarkivet och Rymdstyrelsen att bistå UD-SSSB i uppdraget som nationell säkerhetsmyndighet. Arbetet inom detta område består dels i att UD-SSSB regelbundet samlar företrädare för dessa myndigheter för informationsutbyte och diskussioner i dessa frågor. Berörda myndigheter medverkar också i beredning och förhandlingar i bl.a. Europeiska rådets och ESA:s säkerhetskommitté samt i säkerhetsinspektioner och andra uppdrag.

Enligt Europeiska rådets bestämmelse skall varje medlemsstat upprätta en ”nationell säkerhetsmyndighet”. Denna myndighet ges ett mycket vittomfattande ansvar för:

- att upprätthålla säkerheten för sekretessbelagda handlingar från dessa organisationer vid nationella ministerier, organ eller myndigheter, offentliga eller privata, inom landet eller utomlands,
- att tillåta inrättandet av ett register för uppgifter med beteckningen *Top secret*,
- den periodiska inspektionen av säkerhetsarrangemangen för sekretessbelagda uppgifter,
- att säkerställa att alla medborgare och alla utlänningar som arbetar vid nationella ministerier, organ eller myndigheter

som kan få tillgång till EU-uppgifter som säkerhetsklassas som t*op secret*, *secret* och *confidential* har säkerhetsprövats,
- att utarbeta sådana säkerhetsplaner som anses nödvändiga för att förhindra att sekretessbelagda EU-uppgifter hamnar hos obehöriga.

I Sverige är dessa ansvarsområden fördelade mellan olika myndigheter, som t.ex. Säkerhetspolisen och Förvarsmakten. Regeringen har inte funnit anledning ändra denna redan givna förvaltningsstruktur. Men funktionen som nationell säkerhetsmyndighet påtalar behovet att skapa en kontaktyta mellan EU och berörda svenska myndigheter. Det handlar dels om att bevaka rättsutveckling och annat i vårt land för att Sverige som medlemsstat skall kunna leva upp till kraven att respektera rådets säkerhetsföreskrifter. Dels är det fråga om att utveckla former för att företrädare för vårt land skall kunna delta i säkerhetsorganisationen (säkerhetskommittén) och säkerhetsarbetet inom Europeiska rådet.

Försvarsdepartementets verksamhetsområde

De frågor rörande informationssäkerhet som behandlas inom försvarssektorn är tydligt kopplade till säkerhets- och försvarspolitiska aspekter. Flera av sektorns myndigheter har under 2002 fått ett särskilt ansvar inom informationssäkerhetsområdet, t.ex. Krisberedskapsmyndigheten, Försvarets radioanstalt och Försvarets materielverk. Verksamheten vid dessa myndigheter är under uppbyggnad. Närmare beskrivning av detta finns nedan i detta kapitel. Därtill har Förvarsmakten föreskriftsrätt och tillsynsansvar för vissa totalförsvarsmyndigheter enligt Säkerhetsskyddsförordningen (1996:633).

Informationssäkerhetsfrågorna är ett viktigt område inom försvarssektorn. Detta har sin koppling till att en hel del av verksamheten har beröring med rikets säkerhet under höjd beredskap eller förberedelser för detta. Under de senaste åren har en tyngdpunktsförskjutning mot mer fredstida hot aktualiserat behovet av informationssäkerhet i samhället i stort. Inriktningen har härvid främst varit att skydda kritisk infrastruktur. Detta har lett till att Försvarsdepartementet mer aktivt arbetar med dessa frågor.

I dagsläget finns det på nationell nivå inte någon tydligt formulerad målsättning för informationssäkerhetsfrågorna inom försvarssektorn. Däremot finns det en stomme till strategi uttryckt i proposition 2001/02:158 (se under avsnitt 2.1 ovan). Vidare är en målsättning under utarbetande inom Försvarsdepartementets verksamhetsområde. Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk, Krisberedskapsmyndigheten och Totalförsvarets Forskningsinstitut utgör viktiga aktörer inom området.

Socialdepartementets verksamhetsområde

Tre uppgifter (områden) är centrala inom Socialdepartementets område: a) hälso- och sjukvård, b) socialtjänstsystem och c) socialförsäkringssystem. Det ställs höga krav på att dessa tre områden skall fungera under alla betingelser. Naturligen följer att frågor av integritetskaraktär, betraktat ur ett informationssäkerhetsperspektiv, är intressanta och aktuella för Socialdepartementets verksamhet.

Den 3 april 2003 beslutade regeringen att tillsätta en utredning om nationella kvalitetsregister inom hälso- och sjukvården, m.m. (Kvalitetsutredningen, S 2003:03). Förutom att utreda och lämna förslag till en särskild författningsreglering av kvalitetsregister, har utredaren också fått i uppdrag att se över regionala cancerregister, metadonregister, donationsregister samt utreda förutsättningarna kring tillskapande av vaccinationsregister och blodgivarregister och vid behov lämna förslag till reglering även för dessa. Utredningen skall redovisa sitt arbete till regeringen senast den 30 juni 2004.

Inom Socialdepartementet pågår också förberedelser för att utreda frågor kring behandlingen av personuppgifter inom hälso- och sjukvården. Flera lagar, så som patientjournallagen (1985:562), vårdregisterlagen (1998:544) och sekretesslagen (1980:100), berörs av denna översyn.

Inom hälso- och sjukvården används olika former av IT-stöd i ökande utsträckning. Med hänsyn till det får också IT-säkerhetsfrågor en större betydelse. Hittills finns inte några nationella standarder för IT-säkerhet i hälso- och sjukvården. Främsta orsaken till detta är Sveriges starkt decentraliserade hälso- och sjukvårdssystem, där landstingen beslutar inom sina respektive om-

råden. Det finns därför en mängd olika varianter på hur IT-stöden är utformade i svensk hälso- och sjukvård, med många gånger begränsade möjligheter för systemen att samverka. I takt med den ökade IT-användningen är detta en fråga som aktualiserats allt oftare under senare tid, vilket Socialdepartementet uppmärksammat. Socialdepartementet stödjer därför IT-organisationen Carelink, som gemensamt bildats av Landstingsförbundet, Svenska Kommunförbundet, Apoteket AB, samt de privata vårdgivarna, med pengar från de s.k. Dagmarmedlen.

Inom ramen för Socialdepartementets verksamhet, exempelvis kopplat till socialförsäkringssystemen, hanteras stora belopp i regelbundna transfereringar. Många medborgare är helt beroende av utbetalningar från socialförsäkringssystemet för sin försörjning. Det finns därtill en stor mängd skyddsvärd information.

De till Socialdepartementets område hörande myndigheterna redovisar genomförda risk- och sårbarhetsanalyser samt bedömningar. Socialdepartementet har påtalat att departementet inte tar del av dessa i sin helhet varvid det kan finnas informationssäkerhetsrelaterade problem kopplade till de olika myndigheterna som Socialdepartementet, och därmed den nationella nivån, inte närmare behandlar.

Relevanta aktörer inom Socialdepartementets verksamhetsområde, nationellt och internationellt, är Riksförsäkringsverket, Socialstyrelsen, Läkemedelsverket, Landstingsförbundet samt Apoteket AB.

Finansdepartementets verksamhetsområde

Finansdepartementet har enligt sin arbetsordning ett ansvar för allmänna frågor om statsförvaltningen, vari bl.a. ingår övergripande frågor om informationsteknik inom statsförvaltningen.

Finansdepartementet ansvarar för Statskontoret som enligt sin instruktion skall ”samordna arbetet med den fredstida informationssäkerheten när det rör den civila statsförvaltningen under regeringen och dessutom på begäran och i mån av resurser lämna myndigheterna inom totalförsvaret, riksdagen och dess myndigheter samt de kommunala myndigheterna råd och upplysningar i sådana frå-

gor". En närmare redovisning av Statskontorets arbete med informationssäkerhetsfrågor lämnas i avsnitt 2.1.3

En ny nämnd, Nämnden för elektronisk förvaltning, inrättades den 1 januari 2004. Nämnden, som är administrativt knuten till Statskontoret, har till uppgift att stödja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte mellan myndigheter samt mellan myndigheter och enskilda genom att:

- besluta om de standarder eller liknande krav som skall vara gemensamma för det elektroniska informationsutbytet för myndigheter under regeringen,
- bistå med information och utarbeta riktlinjer, samt
- verka för att det på informationsteknikmarknaden tillhandahålls tjänster och produkter till stöd för elektroniskt informationsutbyte.

Finansdepartementet ansvarar även för Datainspektionen, som inom ramen för sitt tillsynsansvar för bl.a. personuppgiftslagen har tagit fram allmänna råd för säkerhet för personuppgifter. Ansvaret för personuppgiftslagen ligger på Justitiedepartementet. En närmare redovisning av Datainspektionens arbete med informationssäkerhetsfrågor lämnas i avsnitt 2.1.3.

Inom ramen för Finansdepartementets allmänna ansvar för frågor om statsförvaltningen har ett omfattande utvecklingsarbete initierats genom regeringens förvaltningspolitiska handlingsprogram. Ett viktigt inslag i detta arbete är utvecklingen av en elektronisk förvaltning och s.k. 24-timmarsmyndigheter, dvs. myndigheter som är elektroniskt tillgängliga dygnet runt överallt. En elektronisk förvaltning förutsätter betryggande säkerhetslösningar, varför informationssäkerhetsfrågor har en central roll i detta utvecklingsarbete.

Särskilda insatser har gjorts för att säkra förvaltningens tillgång till säkra system för elektronisk identifiering och signering. Skatteverket har under ett inledningsskede haft regeringens uppdrag att i samarbete med Riksförsäkringsverket, Patent- och registreringsverket och Statskontoret ha ett sammanhållande ansvar för detta arbete. Arbetet har bl.a. resulterat i att ramavtal om elektroniska idtjänster slutits med ett antal banker och att riktlinjer utarbetats för elektronisk identifiering och signering.

Även andra insatser görs inom ramen för Statskontorets arbete för att åstadkomma en säker och effektiv infrastruktur för den statliga förvaltningens elektroniska kommunikation och ärendehantering.

Inom ramen för EU-samarbetet ansvarar Finansdepartementet med biträde av Statskontoret för den svenska medverkan i ett program för datautbyte mellan förvaltningar, det s.k. IDA-programmet . Inom ramen för detta program pågår bl.a. en utveckling av säkra nättjänster för kommunikationen mellan EU:s institutioner och medlemsstaternas förvaltningar.

Jordbruksdepartementets verksamhetsområde

En politisk strävan har varit att myndigheter skall erbjuda en god kvalificerad service via Internet. Detta innebär bl.a. att allt som går att publicera via nätet, också skall finnas åtkomligt där. Inom Jordbruksdepartementets verksamhetsområde finns inget annat uttalande som direkt härrör sig till informationssäkerhet.

Jordbruksdepartementet ansvarar för 16 myndigheter. Dessa myndigheter har i sina organisationer egna informationschefer som också hanterar respektive myndighets informationssäkerhet. Det finns ett väl etablerat nätverk mellan myndigheternas informationschefer och Jordbruksdepartementets informationschef, och inom detta nätverk diskuteras också informationssäkerhetsfrågor.

I regleringsbreven till myndigheterna finns den politiska inriktningen att det skall finnas en god kvalificerad service via Internet angiven. I de fall brister har uppstått inom detta område, har departementet vidtagit åtgärder, bl.a. genom att ge myndigheterna i uppdrag att se över problemet.

Departements myndigheter har väl uppbyggda kontakter med näringslivet. I samverkan med näringslivet diskuteras främst frågor som berör myndigheterna och dessas ansvarsområden. Ett exempel är Jordbruksverkets projekt STUDS (Större utbrott av smittsamma djursjukdomar), som pågick mellan oktober 2002 och juni 2003. Inom ramen för projektet byggdes ett nätverk mellan myndigheter, organisationer och företag upp, bl.a. i syfte att utbyta information. Ambitionen är att detta nätverk skall bibehållas genom den sam-

verkansgrupp med representanter från myndigheter och näring som bildats för att fortsätta det strategiska arbetet med beredskap, och däribland informationssäkerheten.

Näringsdepartementets verksamhetsområde

Av de frågor som Näringsdepartementet enligt arbetsordningen ansvarar för är följande intressanta för utredningen: elektronisk handel, elektronisk kommunikation och infrastruktur för informationsteknik. Arbetsordningen ger också departementet ansvar för frågor om användningen av informationsteknik som inte hör till något annat departement.

Näringsdepartementet ansvarar för lagen (2003:389) om elektronisk kommunikation och lagen (2000:832) om kvalificerade elektroniska signaturer som båda berör informationssäkerhet.

Post- och telestyrelsen är den myndighet som arbetar med dessa lagar och en rad andra frågor som rör informationssäkerhet och elektronisk kommunikation (se vidare under avsnitt 2.1.3).

Ett centralt politikområde är elektronisk kommunikation. Riksdagen tog den 5 juni 2003 beslut om lag om elektronisk kommunikation (prop. 2002/03:110, bet 2002/03:TU6, rskr. 2002/03:228). Den nya lagen utgår från EG-reglering vars övergripande målsättning är att åstadkomma ett harmoniserat regelverk för elektroniska kommunikationsnät och elektroniska kommunikationstjänster samt tillhörande installationer och tjänster. Bakgrunden till den nya regleringen är utvecklingen inom området, vilken innebär att olika infrastrukturer och tekniker för överföring av kommunikation sammansmälter. Detta har skapat behov av en samordnad och teknikneutral lagstiftning. Marknadens utveckling har också medfört en önskan om en mer flexibel reglering. En bärande tanke bakom det nya regelverket är att konkurrensfrämjande särlagstiftning endast skall användas om behov föreligger. Den nya lagen trädde i kraft den 25 juli 2003 och ersätter telelagen (1993:597) och lagen (1993:599) om radiokommunikation. (Se vidare kapitel 3 Författningar.)

Näringsdepartementet ansvarar för flera myndigheter, affärsverk och bolag som har betydelse inom informationssäkerhetsområdet,

t.ex. elkraftförsörjning, luftfart, sjöfart, järnvägs- och vägtransporter. Dessa innehar olika roller som användare av viktiga IT-system, leverantörer av samhällsviktiga tjänster, tillsyn och reglering m.m.

Den politiska inriktningen av det arbete som bedrivs inom Näringsdepartementets verksamhetsområde har som utgångspunkt regeringens IT-proposition – Ett informationssamhälle för alla (prop. 1999/2000:86, bet. 1999/2000:TU9, rskr. 1999/2000:256). Regeringen skrev bl.a. att tilliten till information och informationssystem är viktig för tillväxt och konkurrenskraft i den ekonomi som nu utvecklas. I propositionen prioriterade regeringen följande informationssäkerhetsområden: a) skydd mot informationsoperationer, b) ett säkrare Internet samt c) elektroniska signaturer och annan säkerhetsteknik. I propositionen understryker regeringen också att det är viktigt att Sverige spelar en aktiv roll i det internationella arbetet.

Näringsdepartementet arbetar med flera internationella frågor. Inom EU har beslut fattats om flera resolutioner om informationssäkerhet och t.ex. förordningen om den europeiska nät- och informationssäkerhetsbyrån (Enisa). De direktiv som ligger till grund för de ovan nämnda lagarna har också varit departementets ansvar under förhandlingarna i rådet.

Utöver EU har departementet ansvar för frågor om OECD och ICANN (The Internet Corporation for Assigned Names and Numbers). OECD har t.ex. beslutat om nya riktlinjer för nät- och informationssäkerhet. ICANN har ett samordningsansvar vad gäller Internets adressystem. Inom ICANN finns GAC (Governmental Advisory Committee), en rådgivande kommitté för stater, distinkta ekonomier och internationella organisationer. Viktiga frågor för departementet är en internationalisering av Internetarbetet med bibehållen innovationsförmåga. Flera säkerhetsfrågor behandlas i ICANN-processen. (För ytterligare information om ICANN, se kapitel 4 Internationella trender.)

2.1.3 Myndigheternas uppgifter och verksamhet inom informationssäkerhetsområdet

I detta avsnitt presenteras ett antal myndigheters verksamhet inom informationssäkerhetsområdet. Beskrivningarna baseras i huvudsak

på underlag från myndigheterna och utredningen gör i detta sammanhang ingen värdering av den redovisade inriktningen och verksamheten. Myndigheterna är inte rangordnade utan presenteras i enlighet med ordningsföljden i statskalendern. (Försvarshögskolan och Totalförsvarets forskningsinstitut behandlas i kapitel 5 Kompetensförsörjning).

Åklagarväsendet

I sin verksamhet för att utreda och beivra brott kommer åklagarna allt oftare i kontakt med IT-relaterade frågor. IT används i stor omfattning som redskap när brott begås. Det förekommer också utredningar om angrepp mot IT-system. Det finns dock ett stort mörkertal, eftersom de som utsätts kan vara obenägna att anmäla intrång, exempelvis inom finansmarknaden, då det skulle kunna skada tilltron om detta blev känt. Bevissäkring i IT-miljö är ett annat viktigt område. I slutet av 1990-talet började Riksåklagaren därför att utbilda särskilda IT-åklagare. Efterhand har man emellertid kunnat konstatera att IT-relaterade frågor har så stor betydelse att alla åklagare med specialistkompetens inom något område måste ha särskild kunskap när det gäller IT. Särskild IT-utbildning ingår därför i den basutbildning som alla specialiståklagare får.

Polisen

Uppgift
Polisen har till uppgift bl.a. att förebygga brott samt att bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Det innebär att polisen har en central roll när det gäller att ingripa mot informationsrelaterade hot och angrepp, eftersom sådana nästan alltid innebär att angriparen gör sig skyldig till någon form av brott. De brott som i första hand blir aktuella är brytande av post- eller telehemlighet enligt 4 kap. 8 §, dataintrång enligt 4 kap. 9 c § och s.k. datorbedrägeri enligt 9 kap. 1 § 2 st brottsbalken.

Polisen har också en viktig roll när det gäller säkerhetsskydd. Polisen ansvarar bl.a. för genomförande av registerkontroll för säkerhetsprövning, rådgivning, kontroll av myndigheternas säkerhetsskydd samt utfärdande av verkställighetsföreskrifter rörande säkerhetsskyddslagen.

För att utreda informationsrelaterade brott används olika arbetsmetoder och tvångsmedel. I lagen om elektronisk kommunikation finns bestämmelser om polisens rätt att få tillgång till historiska trafikuppgifter. I rättegångsbalken finns bestämmelser bl.a. om beslag samt hemlig teleavlyssning och hemlig teleövervakning. Särskild kompetens för att utreda brott i IT-miljö finns vid Rikskriminalpolisen och Säkerhetspolisen, vid vissa regionala polismyndigheter samt vid Ekobrottsmyndigheten och Statens kriminaltekniska laboratorium.

Verksamhet
Inom Rikskriminalpolisen finns en IT-brottsrotel som skall biträda polismyndigheterna operativt bl.a. med Internetspaning och säkring av digital bevisning, samt svara för samverkan med näringslivet liksom för samordning mellan polismyndigheter och andra myndigheter avseende ärenden, underrättelser och brottsförebyggande åtgärder. IT-brottsroteln skall också – i samverkan med andra delar av polisväsendet – bedriva utbildning samt teknik- och metodutveckling. Roteln har ett nära samarbete med Säkerhetspolisen, regionala IT-brottsutredare och Statens kriminaltekniska laboratorium. Roteln deltar även i internationell verksamhet bl.a. inom Interpol och Europol samt samverkar med sina utländska motsvarigheter. Roteln har en operativ dygnetruntberedskap och är Sveriges kontaktpunkt inom ramen för G8-överenskommelsen.

Säkerhetspolisen leder och bedriver polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet, samt terrorismbekämpning. Säkerhetspolisen fullgör också Rikspolisstyrelsen uppgifter enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen. Genom kontroll, rådgivning och information till myndigheter och företag verkar Säkerhetspolisen för att skapa och vidmakthålla ett tillfredsställande säkerhetsskydd. I kontroll- och rådgivningsverksamheten är IT-säkerhet en viktig del. I regeringens riktlinjer för Säkerhetspolisens verksamhet 2004 anges när det gäller säkerhetsskydd bl.a. att rådgivning också skall ges till de myndigheter och företag som – utan att en fråga direkt avser rikets säkerhet – har ett särskilt ansvar för att förhindra uppkomsten av svåra påfrestningar på samhället i fred. Frågor som rör informationssäkerhet i IT-miljö skall, enligt riktlinjerna, särskilt uppmärksammas och det arbetet skall bedrivas som en integrerad del av verksamheten. Inom säkerhetsskyddet bedrivs även omvärldsanalys för att följa

och analysera nationella och internationella trender som kan påverka säkerhetsskyddsarbetet, med särskild inriktning på informationssäkerhet. Säkerhetspolisen samarbetar med olika polis- och säkerhetsorganisationer, såväl nationellt som internationellt, deltar i andra nätverk på informationssäkerhetsområdet och föreläser ofta vid utbildningar på området. Även inom Säkerhetspolisen bedrivs teknik- och metodutveckling, bl.a. när det gäller säkring av bevis i form av IT-lagrad information. Säkerhetspolisen har vidare inom polisen ansvar för verkställighet av beslut om hemlig teleavlyssning och hemlig teleövervakning.

Eftersom det i ett inledningsskede ofta är oklart vad som är syftet med ett misstänkt IT-angrepp och vem som ligger bakom, har Polisen inrättat en samordningsfunktion med organisatorisk placering vid Rikskriminalpolisens IT-brottsrotel. 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. Den är en central kontaktpunkt för de utredningsresurser som finns vid polismyndigheterna och Statens kriminaltekniska laboratorium i frågor rörande incidenter, brottsmetoder och bevissäkring i IT-miljö m.m. Funktionen skall också ha lägesöverblick och bedriva kriminalunderrättelseverksamhet. Den utgör polisens kontaktyta mot andra aktörer i samhället som har uppgifter inom informationssäkerhetsområdet och kommer att bedriva brottsförebyggande verksamhet genom bl.a. föreläsningar och utbildningar, samt sammanställa och sprida information.

Styrelsen för ackreditering och teknisk kontroll

Uppgift
Styrelsen för ackreditering och teknisk kontroll (SWEDAC) är en myndighet under Utrikesdepartementet, som har till uppgift att verka som nationellt ackrediteringsorgan, samt att samordna, övervaka, ge råd om och informera i kontrollfrågor enligt lagen om teknisk kontroll.

Verksamhet
Certifiering av Ledningssystem för informationssäkerhet mot SS 62 77 99-2 (BS 7799-2) handlar om att skydda en organisations informationstillgångar och att säkerställa att verksamheten kan be-

drivas i kontinuitet. Detta skapar förtroende hos verksamhetens intressenter.

För att få jämförbar nivå på utfärdade certifikat inom exempelvis informationssäkerhetsområdet, finns det standarder och riktlinjer för hur certifieringsorganen bör vara organiserade och bedriva sin verksamhet. I Sverige utfärdas ackreditering av certifieringsorgan inom området ledningssystem för informationssäkerhet av Styrelsen för ackreditering och teknisk kontroll. Motsvarande system finns i de flesta industriländer.

Styrelsen för ackreditering och teknisk kontroll är medlem i Common Criteria Recognition Arrangement (CCRA) vilket innebär att utfärdade certfikat i Sverige blir ömsesidigt erkända i alla andra medlemsländer. Styrelsen för ackreditering och teknisk kontroll (SWEDAC) som är nationell signatär, representerar Sverige i CCRA.

Styrelsen för ackreditering och teknisk kontroll deltar i det europeiska arbetet kring harmonisering av regelverket kring elektroniska signaturer. En viktig del av detta arbete bedrivs inom Forum of European Supervisory Authorities for Electronic Signatures (FESA).

En annan viktig del av myndighetens verksamhet är bedömning av informationssäkerheten hos medicinska laboratorier och dess elektroniska distribution av provrapporter etc. Detta är idag en integrerad del vid ackreditering av dessa högteknologiska och komplexa laboratorier.

Försvarsmakten

Uppgift
Försvarsmaktens uppgift inom området militära informationsoperationer och informationssäkerhet är att ha förmåga att möta olika former av informationsoperationer och därigenom bidra till samhällets totala motståndsförmåga. Även övriga uppgifter som Försvarsmakten har kan beröra informationsoperationer och informationssäkerhet.

Verksamhet
Försvarsmakten har följande mål inom området militära informationsoperationer: Försvarsmakten skall ha förmåga inom de aspekter som omfattas av begreppet informationsoperationer. Försvarsmakten skall utgöra en operativ resursbas för samhället i övrigt avseende informationsoperationer, i enlighet med ställda uppgifter till Försvarsmakten.

Inom Försvarsmakten används begreppet informationsoperationer med följande innebörd: Informationsoperationer är samordnad verksamhet som genomförs i syfte att påverka motståndarens eller andra aktörers beslut. Detta uppnås genom att påverka beslutsfattare, informationsbaserade processer och system, samtidigt som egna beslutsfattare, informationsbaserade processer och system skyddas. Informationsoperationer stödjer aktivt egna defensiva och offensiva syften.

Försvarsmakten utvecklar sin förmåga att motstå informationsoperationsangrepp genom att en organisatorisk enhet skapats som har det övergripande funktionsansvaret avseende informationsoperationer (IO). Enheten samordnar utvecklingen av Försvarsmaktens samlade förmåga inom informationsoperationer där verkansförmågor som elektronisk krigföring (inklusive telekrigföring, Computer Network Operations samt övrig signalkrigföring), PSYOPS, vilseledning och fysisk bekämpning ingår. Grundläggande förmågor som stödjer detta är bl.a. förmåga inom Information Assurance, underrättelser samt operationssekretess. Försvarsmakten har skapat en militärstrategisk inriktning avseende informationsoperationer, Försvarsmaktens Grundsyn IO. Nya förbandstyper som bidrar till förmågan inom informationsoperationsområdet är exempelvis FM CERT, IT-försvarsförband, och telekrigsförband.

Det åligger Försvarsmakten att leda och bedriva militär säkerhetstjänst, samt att leda och samordna totalförsvarets signalskyddstjänst, som även den är en säkerhetsskyddsangelägenhet.

För Försvarsmakten är en väl fungerande signalskyddstjänst en förutsättning för verksamheten. Försvarsmakten är för närvarande och under överskådlig framtid den största användaren av såväl enkla som avancerade kryptolösningar i statsförvaltningen. Införandet av Nätverksbaserat försvar kommer att ställa än högre krav på signalskydd.

Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som främst berör Försvarsmakten och att bl.a. biträda polisen i dess ansvar beträffande skydd av rikets säkerhet. Säkerhetsintressena omfattar eller kan hänföras till personal, materiel, anläggningar, information samt planering och planer i vid bemärkelse.

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Säkerhetsunderrättelsetjänstens uppgift är att klarlägga den säkerhetshotande verksamhetens omfattning, inriktning samt medel och metoder. Säkerhetsskyddet omfattar informations- och IT-säkerhet, tillträdesbegränsning, säkerhetsprövning, utbildning och kontroll.

Vad gäller ledning och samordning av signalskyddstjänsten har Försvarsmakten föreskrifts- och tillsynsansvar för statliga myndigheter. Försvarsmakten ansvarar därmed för utveckling och godkännande av signalskyddssystem, produktion och distribution av kryptonycklar samt Totalförsvarets PKI-tjänst (Public Key Infrastructure). Försvarsmakten lämnar ett omfattande stöd till Regeringskansliet samt EU:s rådssekretariat avseende signalskyddstjänst.

Försvarsmaktens ansvarsområde inom IT-säkerhetsområdet omfattar de myndigheter för vilka Försvarsmakten har föreskrifts- och tillsynsansvar, dvs.: Försvarsmakten, Försvarshögskolan, Försvarets materielverk, Totalförsvarets forskningsinstitut, Fortifikationsverket, Pliktverket och Försvarets radioanstalt.

Försvarsmakten vidareutvecklar övervakningsfunktionen för egna datanätverk och IT-system (FM CERT). Övervakningen inriktas på att säkerställa sekretess, tillgänglighet, riktighet och spårbarhet. FM CERT ingriper och stödjer vid IT-relaterade incidenter inom Försvarsmakten och hos tillsynsmyndigheterna.

För att inrikta och prioritera säkerhets- och signalskyddet tar Försvarsmakten fram en hot- och riskbild. Denna innefattar både hotbild i form av aktörer, viljor, förmågor och sårbarheter hos försvarets och totalförsvarets IT-infrastruktur och IT-system. Regelverket utformas utifrån hot- och riskbilden.

Försvarsmakten har nyligen utkommit med en omarbetad version av Försvarsmaktens föreskrifter om säkerhetsskydd, i syfte att skapa ett mer balanserat och internationellt anpassat skydd med fyra informationssäkerhetsklasser: *hemlig/restricted, confidential, secret* och *top secret*. Försvarets Författningssamling (FFS) för signalskydd är under omarbetning och beräknas vara klar juni 2004.

En viktig del i informationssäkerhetsarbetet är den utbildning som Försvarsmakten bedriver för personal i totalförsvaret på bl.a. Totalförsvarets Signalskyddsskola och Underrättelse- och Säkerhetscentrum.

Försvarsmakten har för att lösa sina uppgifter inom bl.a. hotbildsarbete, IT-säkerhetsmekanismer och utveckling av kryptosystem ett omfattande internationellt samarbete. Delar av detta arbete ställer krav på mycket hög sekretess.

Försvarets materielverk

Uppgift
Försvarets materielverk har i uppgift att anskaffa, vidmakthålla och avveckla materiel och förnödenheter på uppdrag av Försvarsmakten och därvid inom detta område stödja Försvarsmaktens verksamhet. Myndigheten biträder Försvarsmakten i fråga om långsiktig materielförsörjningsplanering samt materielsystemkunskap.

Försvarets materielverk är också patentorgan för de myndigheter som hör till Försvarsdepartementet och handlägger ärenden som rör immaterialrättsliga frågor.

Myndigheten får inom sitt verksamhetsområde även tillhandahålla tjänster åt andra än myndigheter under Försvarsdepartementet och har rätt att ta ut avgifter för sin verksamhet.

Verksamhet
Försvarets materielverk bedriver en omfattande verksamhet som i huvuddelar berör materielförsörjning. Nedan beskrivs de delar av verksamheten som har koppling till informationssäkerhetsområdet.

Försvarets materielverk leder på uppdrag av Försvarsmakten och Krisberedskapsmyndigheten studier, utveckling, upphandling och

verifiering av signalskyddsmateriel och annan säkerhetsrelaterad materiel. Materieluppdragen omfattar ofta säkerhetskrav; detta rör i synnerhet lednings- och kommunikationssystem. Av särskild betydelse är för närvarande utvecklingen av säkerhetsegenskaper i Försvarsmaktens framtida ledningssystem (FMLS) inom ramen för arbetet med det nätverksbaserade försvaret (NBF).

Som patentorgan för myndigheter under Försvarsdepartementet hanterar Försvarets materielverk ofta frågor som berör patentansökningar inom krypteringsområdet.

Myndigheten bedriver vidare teknisk underrättelsetjänst på uppdrag av Regeringskansliet och Försvarsmakten, samt stödjer andra myndigheter med viss information. Delar av detta berör informationssäkerhetsområdet.

I propositionen Samhällets säkerhet och beredskap (2001/02:158) gav regeringen Försvarets materielverk i uppgift att bygga upp ett system för certifiering och evaluering av IT-säkerhetsprodukter. Uppbyggnad av certifieringsfunktionen pågår bl.a. med rekrytering, utbildningsinsatser samt uppbyggnad av regelverk och processer för certifiering. Första provcertifiering kommer att ske under 2004. Uppbyggnaden sker med målsättningen att Försvarets materielverk på sikt skall bli internationellt erkänt som certifieringsorgan inom ramen för den internationella överenskommelsen angående erkännande av IT-säkerhetscertifikat (Common Criteria Recognition Arrangement). Uppbyggnadsarbete sker därvid med utgångspunkt från redan existerande system i de ledande industriländerna.

Försvarets materielverk deltar i ett antal sammanhang på informationssäkerhetsområdet bl.a. vad gäller nationell och internationell standardisering.

Försvarets materielverk har även andra uppgifter med beröring till informationssäkerhetsområdet. Myndigheten bedriver bl.a. kontroll av säkerheten vid leverantörer till Försvarets materielverk inom ramen för upprättade säkerhetsskyddsavtal vid upphandling (SUA) enligt säkerhetsskyddslagen. Försvarets materielverk kan även träffa avtal om säkerhetsskydd med ett svenskt företag om det är nödvändigt för att företaget skall kunna delta i internationellt samarbete om utveckling eller produktion av försvarsmateriel.

Försvarets materielverk deltar också i materielsamverkan och informationsutbyte med andra länders försvarsmyndigheter. Delar av denna samverkan avser informationssäkerhet.

Myndighetens sakkunskap har använts av Regeringskansliet i internationella sammanhang, särskilt inom EU.

Försvarets radioanstalt

Uppdrag
Uppdrag inom kryptosäkerhetsområdet för Försvarets radioanstalt dateras från 1981 då regeringen beslöt att myndigheten skulle ha ett övergripande ansvar för kompetens avseende kryptologi såväl för signalspaningsverksamheten som för totalförsvarets kryptosäkerhetsuppgifter. Försvarets radioanstalt skulle på så sätt stå som garant för att kunskapsbasen och den personliga kompetensen hölls på en hög nivå och därmed bidrog till hög säkerhetsnivå i svenskt signalskydd.

Ett viktigt argument för bildandet av den så kallade kryptologpoolen mellan Försvarets radioanstalt och Totalförsvarets signalskyddsavdelning (TSA) var att känslig kunskap om angreppssätt som Försvarets radioanstalt i sin forceringsverksamhet kunnat utveckla på ett säkert sätt, måste kunna föras över för att gardera svenska krypton mot liknande angreppssätt. Motsvarande argument gäller också för Försvarets radioanstalts kompetens avseende övrig informationssäkerhet.

Försvarets radioanstalt fick i proposition 2001/02:158 ytterligare ansvar inom informationssäkerhetsområdet. Uppgiften enligt myndighetens instruktion är att ha hög teknisk kompetens inom informationssäkerhetsområdet. Försvarets radioanstalt får efter begäran stödja statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Uppgifterna för Försvarets radioanstalt är att:

- stödja insatser vid nationella kriser med IT-inslag,
- medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system,

- genomföra IT-säkerhetsanalyser och
- ge annat tekniskt stöd.

Försvarets radioanstalt skall samverka med andra organisationer inom informationssäkerhetsområdet, såväl inom som utom landet.

Verksamhet
Inom det kryptologiska området bedriver Försvarets radioanstalt forskning och utveckling, samt ett omfattande analytiskt arbete. Merparten av resurserna organiseras inom signalspaningsverksamheten. Härutöver finns ett antal kryptologer som är placerade på Totalförsvarets signalskyddsavdelning. Säkra former finns för hantering av hemlig information såväl från signalspaningen som från kryptosäkerhetsgranskningarna. Modellen med nära samarbete mellan kryptoforcering och signalskydd är avgörande för ett högkvalitativt signalskydd.

Den kryptologiska kompetensen hos Försvarets radioanstalt utnyttjas även i andra sammanhang bl. a. som stöd för Utrikesdepartementet och Inspektionen för strategiska produkter (ISP) samt som sakkunskap vid internationell samverkan, särskilt i EU-frågor. Det senare gäller hela informationssäkerhetsområdet, inte bara det kryptologiska området.

Den verksamhet som byggdes upp under 2003 i samband med myndighetens nya uppgifter är indelad i fyra projekt; krisberedskapsprojektet, forskning och utveckling, konsultverksamhet samt metod och kvalitet.

Krisberedskapsprojektets huvudmål är att ta fram en krisberedskapsplan med interna och externa policy och rutiner som skall användas vid t.ex. en nationell kris med IT-inslag. Efter diskussioner inom ramen för samverkansgruppen för informationssäkerhet, bedömer Försvarets radioanstalt att även den övergripande kunskapen inom informationssäkerhetsområdet behöver utnyttjas. I arbetet med aktiva IT-säkerhetsanalyser upptäcker myndigheten ofta brister avseende policy och rutiner hos kunderna. Genom att bistå med en bredare kompetens inom informationssäkerhetsområdet kan Försvarets radioanstalt ge den enskilda kunden det stöd den behöver för att på ett säkert sätt kunna hantera information i samhällsviktiga system.

Kunder vänder sig till Försvarets radioanstalt för att de har känsliga system som de inte vill, eller anser sig kunna, blottlägga för privata aktörer. Genom att få stöd från Försvarets radioanstalt i en inledande verksamhetsanalys, kan kunden själv prioritera de insatser som är nödvändiga för ett säkerställande av driften. Detta i sin tur leder till att myndigheter kan upphandla konsulttjänster av näringslivet.

Inom ramen för projektet Forskning och Utveckling arbetas huvudsakligen med att söka efter och analysera säkerhetshål. Projektet skapar verktyg för leverans av konsulttjänster och till den attackplattform som används för aktiv IT-kontroll, dvs. penetrationstester. Konsultverksamheten på Försvarets radioanstalt har hittills främst rört aktiva IT-kontroller.

Krisberedskapsmyndigheten

Uppgift
Krisberedskapsmyndighetens uppdrag är att ha det sammanhållande myndighetsansvaret för samhällets informationssäkerhet. I detta ingår att följa upp och utvärdera informationssäkerheten i samhället samt att årligen lämna en rapport till regeringen. Myndigheten har också i uppgift att tillse att det utvecklas ett samarbete mellan offentlig sektor och det privata näringslivet inom informationssäkerhetsarbetet. Uppgifterna till Krisberedskapsmyndigheten är enligt förordning (2002:518) med instruktion för Krisberedskapsmyndigheten formulerade på följande vis:
Krisberedskapsmyndigheten skall enligt 5 § ha ett sammanhållande myndighetsansvar för samhällets informationssäkerhet genom att sammanställa en helhetsbild av informationssäkerheten. Myndigheten skall i detta arbete

1. analysera omvärldsutvecklingen inom området mot bakgrund av erhållet underrättelseunderlag och årligen lämna en samlad bedömning till regeringen,
2. utveckla samarbetet mellan offentlig sektor och näringsliv,
3. arbeta förebyggande med utbildning och information i dessa frågor.

Av 6 § framgår att Krisberedskapsmyndigheten skall utveckla och förvalta tekniskt stöd för ledning och beslutsfattande. Myndighe-

ten skall även samordna signalskyddsverksamheten inom sitt verksamhetsområde.

Enligt 8 § skall Krisberedskapsmyndigheten ha förmåga att vid sådana krissituationer som avses i 1 §, kunna bistå Regeringskansliet med främst områdesvisa lägesbeskrivningar.

I budgetpropositionen 2003/04:1 Utgiftsområde 6[6] ges Krisberedskapsmyndigheten det övergripande ansvaret för arbetet med informationsoperationer[7].

Verksamhet
Krisberedskapsmyndighetens arbetar enligt den givna inriktningen. Myndigheten bedriver följande verksamhet:

- Utövar ett sammanhållande myndighetsansvar.
- Sammanställer en helhetsbild av informationssäkerheten genom egen omvärldsbevakning med stöd av information från underrättelse- och säkerhetsmyndigheten, andra relevanta organisationer samt från näringslivet.
- Utvecklar former och metoder för att, utifrån helhetsbilden, årligen lämna en lägesrapport till regeringen samt att ha förmåga att bistå regeringen med lägesbeskrivningar vid krissituationer.
- Initierar och bedriver samverkan mellan berörda myndigheter och näringsliv samt övriga aktörer inom området.
- Studerar, följer och informerar om den internationella och nationella utvecklingen inom området samt arbetar förebyggande med utbildning och information.
- Utformar rekommendationer för IT-säkerhet mot bakgrund av det nya krishanteringssystemet. Där har rekommendationerna formaliserats i Basnivå för IT-säkerhet (BITS).

[6] Kapitel 3.11.8, avsnitt 6:7 Försvarshögskolan: ”Krisberedskapsmyndigheten har fått det övergripande ansvaret för arbetet med informationsoperationer och det ankommer därför på myndigheten att beställa det stöd den bedömer vara nödvändigt.”
[7] Vid en riksdagsinterpellation den 28 mars 2003 (2003/03:222) fastställde Försvarsministern att informationsoperationer ingår som en del av det övergripande begreppet informationssäkerhet. Krisberedskapsmyndigheten har tolkat detta som att myndighetens ansvar inom informationssäkerhetsområdet omfattar ”skydd mot informationsoperationer”. Detta innebär att Krisberedskapsmyndigheten även har ett ansvar anseende skydd mot perceptionsstyrning, t.ex. skydd mot vilseledning och psykologiska operationer. Krisberedskapsmyndigheten ser ett behov av tydliggörande av begreppen och ansvarsförhållanden på detta område.

- Stödjer länsstyrelser, kommuner och landsting i arbetet med att utforma IT-säkerhetspolicy, styrande dokument, instruktioner för den interna IT-säkerheten i enlighet med BITS.
- Utvecklar en analysmetod som stöd för organisationer att göra säkerhetsanalyser av sina IT-system för att skapa robusta system som har en förmåga att klara svåra påfrestningar på samhället.
- Utvecklar och inriktar signalskydd för att säkra civila myndigheters behov av signalskydd. Krisberedskapsmyndigheten deltar i processen för att utveckla nya signalskyddssystem och -utbildningar.
- Anskaffar signalskyddsmateriel för att möjliggöra säkert informationsutbyte mellan olika aktörer vid allvarlig kris och vid höjd beredskap.
- Bidrar till att stärka krishanteringsförmågan hos kommuner, landsting, länsstyrelser och centrala myndigheter samt lämnar stöd till offentliga organ i krissituationer.
- Driver under perioden mars till september 2004 ett projekt avseende Internetrelaterade hot. Syftet med projektet är att kartlägga vilka Internetrelaterade hot och risker som svenska myndigheter och företag kan utsättas för.
- Ansvarar för det nya radiokommunikationssystemet för skydd och säkerhet, Rakel (radiokommunikation för effektiv ledning).
- Genomför under 2004en svensk förstudie av ömsesidiga beroenden i samhällsviktig infrastruktur . Informationssäkerhetsaspekterna kommer att utgöra en viktig del i detta arbete.
- Initierar och stödjer forskning inom informationssäkerhetsområdet.
- Stödjer genom olika aktiviteter kommunerna i deras arbete med att utveckla en starkare ledningsförmåga.

Datainspektionen

Uppgift
Datainspektionen är central förvaltningsmyndighet som har till uppgift att skydda människors privatliv i IT-samhället. Datainspektionen är tillsynsmyndighet enligt bl.a. personuppgiftslagen och har

tillsynsansvar avseende den informationssäkerhet vid behandling av personuppgifter som behövs för att skydda enskildas integritet.

Verksamhet
Datainspektionen har tagit fram allmänna råd, Säkerhet för personuppgifter, som preciserar personuppgiftslagens krav på säkerhet vid behandling av personuppgifter.

Datainspektionen hjälper enskilda personer som råkat ut för integritetskränkningar, följer upp klagomål och gör inspektioner. Stor vikt läggs vid förebyggande arbete, främst information och regelgivning. Råd och hjälp åt personuppgiftsombud prioriteras. Datainspektionen följer och beskriver dessutom utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och deltar i harmoniseringen av säkerhetsarbetet enligt det s.k. dataskyddsdirektivet EG 95/46/EG.

Statskontoret

Uppgift
Statskontorets främsta uppgift är att stödja regeringen i arbetet med att utvärdera, ompröva, styra och effektivisera statlig och statligt finansierad verksamhet. Statskontoret erhåller dels stående uppdrag i instruktion och regleringsbrev, dels fortlöpande uppdrag genom särskilda beslut och överenskommelser.

För informationssäkerhetsområdet sammanfaller instruktionens mandat i nuläget i stort med Krisberedskapsmyndighetens uppgifter och kommer därför att anpassas till den inriktning som varit gällande i praktiken. Detta innebär att myndighetens uppgift inom informationssäkerhetsområdet kopplas till frågor om utveckling och effektivering av förvaltningen.

Verksamhet
Statskontorets informationssäkerhetsarbete har under de senaste tre åren inriktats på förändringsarbetet i offentlig sektor inom ramen för utvecklingen av 24-timmarsmyndigheten. Den ökade inriktningen på e-tjänster över Internet har skapat ett stort behov av samsyn och gemensamma säkerhetslösningar. Att åstadkomma god

säkerhet har uppfattats som en nödvändighet för att kunna dra nytta av möjligheterna med IT för utveckling mot en elektronisk förvaltning. Utredningar avseende elektronisk identifiering och signering, smarta kort, säker e-post, samt incidenthantering har genomförts. Vägledningar avseende informations- och IT-säkerhet allmänt har publicerats. Resurser har naturligtvis också lagts på kravställande avseende säkerhet i samband med upphandling av produkter och tjänster.

Statskontoret kommer att tillhandahålla kanslistöd till Nämnden för elektronisk förvaltning (NEF) som bildades den 1 januari 2004. Nämndens syfte är att ge ut föreskrifter, riktlinjer och vägledningar för det elektroniska informationsutbytet mellan myndigheter, samt mellan myndigheter och enskilda. Nämnden skall stödja utvecklingen av elektronisk förvaltning och tillämpning av elektronisk signering.

Statskontorets insatser har i första hand omfattat:

- Försörjning med elektroniska identiteter, för allmänheten och tjänstemän i offentlig förvaltning, har åstadkommits genom upphandling av bl.a. bankernas id-tjänst (BID) och motsva-rande tjänster från Nordea, Posten AB, TeliaSonera AB och Steria AB. Statskontoret har medverkat i regeringens uppdrag att delta som en part i samarbetet för elektroniska signaturer med Skatteverket, Riksförsäkringsverket och Patent- och registreringsverket (Samset). Samarbetet har bl.a. resulterat i riktlinjer för elektronisk identifiering och signering.
- Formkravsutredningen som resulterade i en rapport med syftet att undanröja onödiga hinder för elektronisk kommunikation och elektronisk dokument- och ärendehantering.
- Utredning och rapport för att belysa arkiveringsproblematiken i samband med användning av digitala signaturer.
- Utformning och upphandling av spridnings- och hämtningssystem (SHS) som är en produkt för att åstadkomma säker datakommunikation mellan myndigheter och mellan myndigheter och andra aktörer (företag, allmänhet).
- Statskontoret har påbörjat ett arbete med att etablera en säker nättjänst för att användas mellan anslutna myndigheter och för säker kommunikation till EU-myndigheter och

andra EU-länders förvaltningar. Den säkra nättjänsten skall vara ackrediterad av svenska säkerhetsmyndigheter och blir därmed den första godkända säkra nättjänsten i svensk statsförvaltning utanför Försvarsmakten, med möjlighet att skicka information som i enlighet med EU:s regler klassificeras som *restricted*.

- Samverkan med informationssäkerhetsansvariga i offentlig sektor genom nätverksaktiviteter. Informationssäkerhetsnätverket (SNITS) behandlar gemensamma frågeställningar och skapar förutsättningar för utveckling av informationssäkerheten.
- Medverkan i Swedish Standards Institute (SIS) projekt Ledningssystem för informationssäkerhet (LIS) som är inriktat på att sprida och förvalta informationssäkerhetsstandarden SS-ISO/IEC 17799.
- Statskontoret har under hösten 2003 publicerat en handbok och ett mallregelverk för informationssäkerhetsarbete enligt ovannämnda standard för 24-timmarsmyndigheter.
- Statskontoret har i enlighet med regeringens proposition 2001/02:158 ställt resurser till förfogande vid etablering och utveckling av samarbetet mellan Krisberedskapsmyndigheten, Post- och telestyrelsen, Försvarets radioanstalt och Försvarets Materielverk.

Post- och telestyrelsen

Uppgift
Post- och telestyrelsen (PTS) är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom postområdet och området för elektronisk kommunikation (förordning 2003:403).

Inom området för elektronisk kommunikation skall Post- och telestyrelsen främja tillgången till säkra och effektiva elektroniska kommunikationer enligt de mål som anges i lagen (2003:389) om elektronisk kommunikation. Myndigheten skall bl.a. följa utvecklingen inom området för elektronisk kommunikation, särskilt vad gäller säkerhet vid elektronisk informationshantering.

Post- och telestyrelsen utövar tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer samt meddelar föreskrifter

enligt förordningen (2000:833) om kvalificerade elektroniska signaturer (förordning 2003:403).

Genom upphandling av samhällsåtaganden får Post- och telestyrelsen tillgodose totalförsvarets behov av elektroniska kommunikationstjänster under höjd beredskap, och stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation och posttjänster i fred (förordning2003:403).

Post- och telestyrelsen har sedan 2001 byggt upp en relativt omfattande verksamhet avseende nät- och IT-säkerhet.

På regeringens uppdrag inrättade Post- och telestyrelsen vid årsskiftet 2002/2003 en rikscentral för IT-incidentrapportering – Sveriges IT-incidentcentrum (Sitic). Sitics uppgift är att stödja samhället i arbetet med skydd mot IT-incidenter. Sitic verkar för att främja informationsutbytet om IT-incidenter mellan samhällets organisationer och sprider information om nya problem som kan störa IT-system. Centrumet lämnar också information och råd om förebyggande åtgärder samt sammanställer och ger ut statistik.

Verksamhet
Sitic har startat sin verksamhet med de 31 myndigheter som är förtecknade i Krisberedskapsförordningen.

Under våren 2003 har arbetet fortskridit med att utveckla samverkansfrågor, lösa juridiska frågor, säkerställa teknisk kompetens och att säkerställa högsta möjliga skyddsnivå i och omkring enheten. Sitic är lokaliserad i en egen sektion på Post- och telestyrelsen med egna system och nätverk med högsta kommunikationssäkerhet. Personalen på Sitic är högt säkerhetsklassade.

I dagsläget har Sitic startat kontinuerlig verksamhet inom samtliga de fyra områden som regeringens uppdrag till Post- och telestyrelsen omfattade:

- Inrätta ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer och funktionen.
- Snabbt kunna sprida information i samhället om nya problem som kan störa IT-system.
- Sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

- Lämna information och råd om förebyggande åtgärder.

Synliga resultat är exempelvis en kontinuerlig publicering av s.k. blixtmeddelanden, särskilda råd och förebyggande råd, liksom en fungerande incidentrapporteringsmekanism.

Inom Internetområdet har Post- och telestyrelsen utfört flera studier och prov avseende Internets robusthet i Sverige. Post- och telestyrelsen verkar även internationellt med särskild tonvikt på säkerhetsfrågor.

Inom områdena totalförsvar och skydd mot svåra påfrestningar i fred samverkar Post- och telestyrelsen aktivt med operatörer och andra myndigheter. Post- och telestyrelsen har bl.a. i partnerskap skapat redundans i bredbandsnät och byggt säkra anläggningar för driftcentraler. Tillsammans med bl.a. Statens energimyndighet och Svenska kraftnät analyseras och åtgärdas det ömsesidiga beroendet mellan el- och telesystemen.

Myndigheten startade i slutet av 2003 kampanjen Surfa säkrare – goda råd och säkerhet på Internet. Kampanjen riktar sig till små och medelstora företagare samt konsumenter.

2.2 Informationssäkerhet i privat sektor och samverkansbehov offentligt - privat

I detta avsnitt ges en kort beskrivning av Föreningen Svenskt Näringsliv, samt två av dess sammanslutningar med anknytning till informationssäkerhetsområdet. Utredningen vill betona att detta inte är en heltäckande beskrivning av informationssäkerhetsarbetet inom den privata sektorn, men då sammanslutningarna har medlemmar från ett brett spektrum inom näringslivet, kan detta dock tjäna som en illustration av det perspektiv på informationssäkerhetsfrågor som finns inom den privata sektorn. Denna beskrivning visar även på den samverkan som successivt växer fram mellan offentlig och privat sektor inom informationssäkerhetsområdet. Utredningen kommer därför i det fortsatta arbete vidare studera den samverkan som finns, ytterligare behov samt vilka effekter detta kan ha. I de tidigare avsnitten har det i myndighetsbeskrivningarna till viss del framkommit vilken samverkan som sker mellan privat och offentlig verksamhet. I detta avsnitt nämns därför endast kort

Krisberedskapsmyndighetens Informationssäkerhetsråd och Svenskt CERT-forum.

2.2.1 Föreningen Svenskt Näringsliv

Föreningen Svenskt Näringsliv bildades år 2001. Inom organisationen finns en avdelning som rymmer säkerhet och företagsjuridik samt konkurrens- och transportfrågor. Även IT-politiska frågor hanteras inom organisationen, t.ex. infrastruktur för fasta och mobila kommunikationstjänster, entreprenörskap och kompetensförsörjning.

Föreningen Svenskt Näringsliv har ca 50 medlemmar (bransch- och arbetsgivarförbund) med ca 57 000 medlemsföretag. Nära samverkan sker med medlemmarna i säkerhetsfrågor, bl.a. inom IT-företagens Informationssäkerhetsråd (se nedan). Föreningen har även genom organisationen Gemenskapen för elektroniska affärer (GEA) drivit informationssäkerhetsfrågor inom arbetsgruppen Tillit och säkerhet.

Föreningen Svenskt Näringslivs grundsyn på säkerhet och riskhantering.

Enligt föreningen Svenskt Näringsliv bör säkerhetsfrågorna ses ur ett riskhanteringsperspektiv – dvs. att helhetssyn är centralt. Informationssäkerheten är – även om den ofta behandlas som en egen disciplin – beroende av andra säkerhetsområden; fysisk säkerhet och skydd av nyckelpersoner kan vara avgörande för skyddets totala effektivitet. Skyddet måste vidare grundas på ett fungerande stöd av lagstiftning och rättssystemet i övrigt.

Internationalisering, ökad IT-användning och nätverkslösningar mellan olika företag har satt fokus på företagens beroende av omvärlden. Kostsamma skadehändelser behöver inte härröra från den egna organisationen eller ens ha sitt ursprung i det egna landet. Företagen delar resurser och därmed sårbarhet beträffande bl.a. infrastruktur som el-, tele-, transport- och betalningssystem samt konsulter, underleverantörer, IT-system och information. Samverkan blir därmed en nödvändighet. Samtidigt visar myndigheternas ärendebalanser och brottsstatistik att företagen i ökad utsträckning

måste ta ansvar för den egna säkerheten. Därför behövs bättre förutsättningar och regler i säkerhetsarbetet, vare sig det gäller insatser mot vardagsbrottslighet eller kvalificerad IT-brottslighet.

Säkerhetsarbetet i företagen har ändrat karaktär. Målet att minimera skador ersätts alltmer av ett bejakande av det s.k. ”medvetna risktagandet” för att därigenom öka affärsmöjligheter och lönsamhet. Eftersom få företag har möjlighet att bygga upp en egen bred kompetens, full informationsbas gällande sårbarheter och hotbild, eller full administrativ stödfunktion inom säkerhetsområdet, får nätverken en ökad betydelse.

En viktig del av företagens säkerhetsarbete är de skyddsstrategier som de använder. Företagen är på många områden helt beroende av de avvägningar de själva gör mellan risk och möjlighet. Beträffande informationssäkerheten blir detta särskilt tydligt. Skyddsåtgärderna måste hela tiden vägas mot värdet av den information som skall skyddas. För att dessa skyddsåtgärder skall kunna fungera som önskat är det dock också nödvändigt att rättsordningen ger stöd. Svenskt Näringsliv betonar exempelvis att det för företagen är viktigt att den information som skyddas som företagshemlighet genom tekniska skyddsåtgärder, också har ett rättsligt skydd genom lagen om skydd för företagshemligheter. Annars finns ingen möjlighet att i praktiken komma åt angrepp på sådan information.

Enligt Svenskt Näringsliv har säkerhetschefens roll också ändrats från operativt skyddsansvarig, till chef för en managementfunktion som stöder affärsverksamhetens riskbedömning, beslutsunderlag och skadehantering. I detta har föreningen Svenskt Näringsliv också en roll som gemensam referensram mellan företag i utvecklingen av företags organisation, kompetensutveckling och styrningsmodeller för säkerhetsarbetet.

Svenskt Näringsliv driver opinionsbildning och förändringsarbete både när det gäller hanteringen av traditionella säkerhetsfrågor som de nya behov som tydliggörs i IT-samhället såsom skyddet av immateriella värden, insatser mot IT-relaterad brottslighet samt balansgången mellan skyddet för medarbetarnas integritet och företagens berättigade krav på fungerande informationssäkerhet. Detta omfattar både nationella och internationella frågor.

2.2.2 Näringslivets Säkerhetsdelegation.

Näringslivets Säkerhetsdelegation (NSD) bildades 1967, och var ursprungligen en tämligen sluten organisation men fungerar idag som ett öppet nätverk för såväl privat som offentlig sektor.

Huvuduppgifterna för organisationen är att vara forum för idé-, erfarenhets- och kunskapsutbyte inom säkerhetsområdet, att bidra till ökat säkerhets- och riskmedvetande bland medlemmar och andra, samt att initiera och driva utvecklingsprojekt.

Arbetet sker i sex regioner, där varje region leds av en ordförande med stöd av en arbetsgrupp. Inom NSD finns en central delegation som koordinerar och ger stöd åt regionernas verksamhet, initierar och driver utvecklingsprojekt, bidrar till kompetensutveckling inom strategiska områden och ger råd till Svenskt Näringsliv i arbetet med säkerhetsfrågor.

Inom NSD bildas vid behov olika arbetsgrupper för längre eller kortare tid. En informationssäkerhetsgrupp har under åren drivit frågor om exempelvis tillgången till fri kryptoteknik och frågan om tillskapandet av en näringslivs-CERT. Andra frågor som hanterats inom andra grupper har gällt exempelvis personlig integritet, mail- och internetpolicy samt personskydd.

Föreningen Svenskt Näringsliv/NSD deltar i och samverkar med exempelvis Krisberedskapsmyndighetens Informationssäkerhetsråd, SIG Security, SIS (gällande Ledningssystem för informationssäkerhet), Swedish Anticounterfeiting Group (SACG), ICC:s data- och telegrupp, Institutet för rättsinformatik (IRI) vid Stockholms universitet samt institutionen för data- och systemvetenskap (gemensam för Stockholms universitet och Kungl. Tekniska högskolan).

Behov uppmärksammade av NSD

Företag måste allt mer ta hand om sina egna säkerhetsbehov genom förebyggande, detekterande och utredande åtgärder. Automatisk säkerhetsbevakning och kontroll är en förutsättning för informationssäkerhetsarbetets praktiska bedrivande. Ofta ifrågasätts dessa åtgärder utifrån att den personliga integriteten riskerar att kränkas.

Näringslivets Säkerhetsdelegation menar att det är viktigt att inte förväxla tillgången till uppgifter (t.ex. till loggar eller inspelningar från kameraövervakning) med hur uppgifterna sedan får användas. NSD menar att goda tekniska säkerhetsåtgärder och administrativa åtgärder är grundläggande förutsättningar för att skydda den personliga integriteten. Dessutom finns direkta krav på företagen att förhindra kriminella och etiskt tvivelaktiga aktiviteter genom verksamhetskontroll (Corporate Governance). Efter att företagens interna utredningar har genomförts krävs att polis, åklagare och domstolar tar vid. Näringslivets Säkerhetsdelegation anser att det på detta område föreligger brister vad gäller resurser, prioritering och förståelse för företagens behov.

Det informationssäkerhetsarbete som bedrivs inom företagen måste grundas på väl fungerande och verklighetsanpassade regelverk, såväl interna regler som lagstiftning. Ändamålsenliga regler som leder till ökad kvalitet och ökad acceptans är en övergripande och viktig fråga även inom säkerhetsarbetet. Enligt NSD upplever många av deras medlemmar bl.a. att de straff- och processrättsliga förutsättningarna för säkerhetsarbetet inte är tillfredsställande. Ett aktuellt exempel är de brister som finns beträffande lagen om skydd av företagshemligheter (FHL). Se vidare under kapitel 3 Författningar och kapitel 6 Utredningens överväganden.

2.2.3 Svenska IT-företagens Organisation (IT-Företagen)

Branschorganisationen IT-Företagen har cirka 550 medlemsföretag inom IT- och telekomområdet. Organisationen verkar för en växande IT-användning i Sverige och ger stöd till enskilda medlemsföretags utveckling, genom att främja affärsmöjligheter, undanröja hinder och tillhandahålla medlemsservice. Frågorna kring informationssäkerhet och tillit har en central roll i organisationens arbete och ett särskilt branschråd har bildats – Informationssäkerhetsrådet. Rådet samlar 35 företag från alla delar av branschen; hård- och mjukvara, tele- och internetoperatörer, telekomleverantörer, systemintegratörer, konsulter och utbildare.

2.2.4 SIG Security – Nationell samverkan för informationssäkerhet (NSi)

SIG Security är en organisation som har över 2000 medlemmar aktiva inom informationssäkerhetsområdet. Organisationen har under 2003 skapat ett forum, Nationell samverkan för informationssäkerhet, med uppgift att verka för ett tryggare informationssamhälle.

2.2.5 Exempel på offentlig-privat samverkan

Krisberedskapsmyndighetens Informationssäkerhetsråd

Krisberedskapsmyndigheten har inom ramen för sitt samordnande ansvar vad gäller informationssäkerhet skapat ett Informationssäkerhetsråd. Informationssäkerhetsrådet har tillsatt en särskild arbetsgrupp för hur näringslivssamverkan skall utvecklas. Arbetsgruppen har konstituerats och för diskussioner kring arbetsformer och medlemmar. Ambitionen är att skapa ett kvalificerat nätverk från näringslivet och arbetsgruppen kommer därför att utökas med fler representanter för olika branscher och kompetensområden.

Svenskt CERT-forum

2003 startades Svenskt CERT-forum, vilket är resultatet av ett gemensamt initiativ från Post- och telestyrelsen/Sitic och Telia CERT. Syftet med Svenskt CERT-forum är att skapa en möjlighet för konkret informations- och erfarenhetsutbyte mellan olika organisationer i samhället som alla har intresse av att bedriva incidenthantering på bästa sätt. Svenskt CERT-forum arrangerar tre halvdagsträffar under året och driver också en gemensam webbplats och diskussionsgrupp.

Post- och telestyrelsen är ordförande för Svenskt CERT-forum. Medlemskap är till för enheter som aktivt arbetar med incidenthantering, både inom näringsliv och den offentliga sektorn. Medlemslistan omfattar bl.a. myndigheter, banker, operatörer och verk-

stadsföretag. Konsulter och produktleverantörer ingår inte i detta sammanhang.

3 Författningar

3.1 Inledning

I regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap anges att regeringen avser låta genomföra en översyn av författningar som berör informationssäkerhetsfrågorna. Inom Justitiedepartementets verksamhetsområde pågår t.ex. en översyn av sekretesslagen, bl.a. för att tillgodose de behov Post- och telestyrelsen (PTS) har för att på ett effektivt sätt kunna bedriva den incidenthanteringsfunktion myndigheten ålagts. En proposition kommer att överlämnas till riksdagen under våren 2004. Vidare bereds för närvarande en departementspromemoria som behandlar några frågor om säkerhetsskyddslagen. Beredningen för rättsväsendets utveckling (BRU) har 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 bl.a. en anpassning och modernisering av rättegångsbalkens terminologi, översyn av vilka verksamheter som bör omfattas av anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning, 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.

I arbetet med informationssäkerhetsfrågorna i relation till lagstiftning, bad utredningen ett antal centrala myndigheter att ge en beskrivning av den nuvarande lagstiftningen, och vilka eventuella hinder som enligt dem ansågs kunna finnas för ett effektivare informationssäkerhetsarbete. Utifrån det underlag som inkom, samt i den närmare dialogen med utredningens sakkunniga och experter fram-

kom att informationssäkerhetsfrågorna berör och berörs av en stor mängd lagstiftning. Vilka begränsningar som föreligger är därmed inte alltid så lätt att överblicka.

I det avslutande kapitlet 6 Utredningens överväganden lyfter utredningen fram ett antal frågeställningar i relation till nu gällande lagstiftning. Som en grund för dessa, och för utredningens fortsatta arbete vad gäller författningsfrågor, presenteras i detta avsnitt ett antal författningar med beröring mot informationssäkerhet. Redogörelsen skall dock inte betraktas som heltäckande.

3.2 Sekretesslagen

I 2 kap. § 1 tryckfrihetsförordningen anges att till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att ta del av allmänna handlingar. Där denna rätt kolliderar med motstående intressen finns möjlighet enligt kapitlets andra paragraf att göra vissa inskränkningar i rätten. Paragrafen anger som motstående intressen som kan motivera en begränsning av allmänhetens rätt att ta del av allmänna handlingar:

1. rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation,
2. rikets centrala finanspolitik, penningpolitik eller valutapolitik,
3. myndigheters verksamheter för inspektion, kontroll eller annan tillsyn,
4. intresset av att förebygga eller beivra brott,
5. det allmännas ekonomiska intresse,
6. skyddet för enskilds personliga eller ekonomiska förhållanden,
7. intresset att bevara djur- eller växtart.

Begränsning av handlingsoffentligheten skall anges i särskild lag, dvs. sekretesslagen, och måste finna stöd i någon av de sju punkterna.

Kapitel 2 i sekretesslagen (1980:100, SekrL) reglerar sekretess med hänsyn till rikes säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation. Första paragrafen reglerar den s.k. utri-

kessekretessen[8] och andra paragrafen den s.k. försvarssekretessen. Det sekretessbelagda området i försvarssekretessen 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 mot 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 t.ex. ett röjande av uppgifter om den civila säkerhetstjänsten vålla fara för rikets säkerhet trots att någon skada för försvaret egentligen inte har inträffat. Viktigt att komma ihåg är att försvarssekretessen gäller inom hela det allmännas verksamhet, även om den har sin största betydelse hos Försvarsmakten och andra myndigheter som ägnar sig åt militär verksamhet och frågor som rör totalförsvaret. På försvarssekretessens område är meddelarfriheten kraftigt inskränkt. Skaderekvisitet för såväl utrikes- som försvarssekretessen är rakt, vilket innebär att offentlighet är huvudregel och sekretessen slår in bara om utlämnande av uppgiften kan antas leda till skada.

Kapitel 5 i sekretesslagen reglerar sekretess med hänsyn främst till intresset att förebygga eller beivra brott. Av 5 kap. § 1 andra stycket framgår att sekretess 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.

Kapitlets andra paragraf anger att sekretess gäller 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,

[8] Uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

4. behörighet att få tillgång till upptagning för automatisk databehandling eller annan handling, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

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 kontrollera 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 t.ex. kryptering som används för att underlätta befordran eller användning av sekretessbelagda uppgifter. Om kryptering används för uppgifter som inte är sekretessbelagda skall även dessa uppgifter kunna hållas hemliga så att chiffret inte kan forceras. Bestämmelsen möjliggör även (p. 2) 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. Däremot saknas skyddskrav på hanteringen av den lika viktiga öppna verifieringsnyckeln som används när signaturens (och därmed dokumentets) äkthet skall kontrolleras. Detta kan illustrera att det kan finnas ett behov av att vidga säkerhetsskyddslagen. Se vidare under kapitel 6 Överväganden.

3.3 Säkerhetsskyddslagen

I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd, med vilket enligt 6 § avses skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet, och skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.

Av 7 § säkerhetsskyddslagen framgår 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 säkerhetssynpunkt deltar i verksamhet som är av betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet skall även i övrigt förebygga terrorism.

Lagen gäller enligt 1 § för staten, kommunerna och landstingen, liksom för bolag som dessa har ett rättsligt bestämmande inflytande över, samt för enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. När staten, kommuner eller landsting skall begära in anbud eller träffa avtal om upphandling, där det förekommer uppgifter som omfattas av sekretess, skall enligt 8 § ett säkerhetsavtal (s.k. SUA-avtal) träffas med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.

Enligt 9 § säkerhetsskyddslagen 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 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, dvs. att uppgifter hämtas från olika polisregister, och i klass 1 och 2 även särskild personutredning. Registerkontroll kan också göras till skydd mot terrorism.

I säkerhetsskyddsförordningen (1996:633) finns närmare bestämmelser om säkerhetsskydd. Enligt 5 § 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 eller skyddet mot terrorism. Resultatet av denna

undersökning (säkerhetsanalys) skall dokumenteras. 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 § säkerhetsskyddsförordningen 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 § 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 där 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 § säkerhetsskyddsförordningen ansvaret för att kontrollera säkerhetsskyddet hos myndigheterna. Rikspolisstyrelsen och Försvarsmakten har vidare, med stöd av 43 – 44 §§ förordningen meddelat verkställighetsföreskrifter för respektive tillsynsområde. I föreskrifterna finns bestämmelser bl.a. om informationssäkerhet.

3.4 Lagen om skydd för samhällsviktiga anläggningar

I lagen (1990:217) om skydd för samhällsviktiga anläggningar (skyddslagen) ges bestämmelser om vissa åtgärder till skydd mot sabotage, terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, spionerі samt röjande i andra fall av hemliga uppgifter som rör totalförsvaret. Lagen ger möjlighet att begränsa tillträ-

det till en anläggning eller ett område genom att förklara det som skyddsobjekt. Som skyddsobjekt får bl.a. förklaras 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. Ett beslut om skyddsobjekt innebär bl.a. att obehöriga inte får tillträde till skyddsobjektet 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, bl.a. mot den som finns skäl att anhålla för spionerі eller sabotage eller förberedelse till sådant brott.

3.5 Brottsbalken

IT används ofta som hjälpmedel vid brott och många brott begås via Internet. Som exempel där IT ofta har 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 således 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.

3.6 Lagen om straff för terroristbrott

Enligt lagen (2003:148) om straff för terroristbrott, döms för terroristbrott den som begår vissa uppräknade gärningar, om gärningen allvarligt kan skada en stat eller en mellanstatlig organisation och avsikten med gärningen är att 1) injaga allvarlig fruktan hos en befolkning eller en befolkningsgrupp, 2) otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från att vidta en åtgärd, eller 3) allvarligt destabilisera eller

förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellanstatlig organisation. Bland de gärningar som under dessa förutsättningar utgör terroristbrott kan nämnas sabotage och grovt sabotage. I förarbetet till lagen nämns ett antal handlingar som under nämnda förutsättningar kan utgöra terroristbrott. Bland dessa kan nämnas förorsakande av, eller hot om utförande av, omfattande förstörelse av infrastruktur och datasystem som kan komma att utsätta människoliv för fara eller förorsaka betydande ekonomiska förluster.

3.7 Lagen om skydd för företagshemligheter (1990:409)

I lagen ges ett allmänt skydd för företagsspecifik information av teknisk, kommersiell och administrativ karaktär, oavsett om den har dokumenterats eller inte. I den inledande paragrafen definieras företagshemlighet som information som näringsidkaren håller hemlig och vars röjande kan medföra skada i konkurrenshänseende. Med företagshemligheter avses i lagen både dokumenterad och erfarenhetsbaserad information. Informationen skall gälla affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig. 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 (företagsspionеri), eller anskaffar en företagshemlighet med vetskap om att den som tillhandahåller företagshemligheten har berett sig tillgång till denna genom företagsspionеri (obehörig befattning med företagshemlighet).

3.8 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.

Syftet med personuppgiftslagen är att skydda människor mot att deras personliga integritet kränks vid automatiserad 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 personuppgiftslagen finns bestämmelser om säkerhet vid behandling av personuppgifter. En tillfredsställande säkerhet är ett krav enligt personuppgiftslagen. Enligt 31 § skall den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter 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 personuppgifterna, och hur pass känsliga de behandlade personuppgifterna är.

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

Ansvaret för säkerheten är enligt personuppgiftslagen den personuppgiftsansvarige, dvs. 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 personuppgiftsbiträde får behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet 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 personuppgifter behandlas automatiserat.

I 9 § personuppgiftslagen finns de grundläggande krav som gäller för behandling av personuppgifter. Där anges bl.a. att den person-

uppgiftsansvarige skall se till att personuppgifter endast samlas in för särskilt uttryckligt angivna ändamål. Uppgifterna får därefter inte behandlas för något ändamål som är oförenligt med det ändamål som de samlades in för. Den personuppgiftsansvarige får inte heller behandla fler uppgifter än vad som är nödvändigt med hänsyn till ändamålet.

Personuppgiftslagen innehåller också regler om i vilka situationer 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 har långtgående krav på att den personuppgiftsansvarige skall informera de registrerade om den behandling av personuppgifter som utförs.

3.9 Lagen (2003:389) om elektronisk kommunikation

Genom lagen om elektronisk kommunikation (EkomL) implementeras fem direktiv och ett beslut i Sverige[9], vilka har beslutats inom EU.

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 bl.a. reglerar integritetsskydd. Av 2 § framgår att personuppgiftslagens bestämmelser skall gälla

[9] Europaparlamentets och rådets direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet). Europaparlamentet och rådets direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet). Europaparlamentet och rådets direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet). Europaparlamentets och rådets direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (direktivet om samhällsomfattande tjänster), Europarlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation), Europarlamentets och rådets beslut nr 676/2002/EG om ett regelverk för radiospektrumpolitiken i Europeiska gemenskapen (radiospektrumbeslutet).

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 3 och 4 §§ framgår 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 tillhandahållande 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, dvs. inte drifts- och funktionssäkerhet.

I 6 kap. 5-10 §§ regleras behandling av trafikuppgifter och lokaliseringsuppgifter. 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, t.ex. 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, t.ex. 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 m.m. Samtycket kan när som helst återkallas.

I 6 kap. 15-16 §§ EkomL återfinns bestämmelser om abonnentuppgifter 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 upptas 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 § EkomL 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 § 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 raderat uppgifterna. För närvarande finns inte någon skyldighet att spara trafikuppgifter för de brottsutredande myndigheternas verksamhet.

4 Internationella trender

I detta avsnitt ges en övergripande bild av utvecklingen av informationssäkerhetsarbetet i andra länder. Därefter görs en beskrivning av arbetet med dessa frågor inom ramen för OECD och EU. Avslutningsvis behandlas kortfattat ett antal andra internationella forum av betydelse inom informationssäkerhetsområdet. Utredningen vill betona att detta inte skall betraktas som en i alla sammanhang heltäckande beskrivning.

Utredningen har för avsikt att i slutrapporten behandla de internationella aspekterna utförligare. I samband med slutrapporten, när utredningen lägger fram sina förslag och en mer grundlig analys presenteras, kommer det internationella perspektivet att på ett tydligare vis användas som jämförelseunderlag och integreras i den övergripande analysen.

4.1 Utvecklingen i andra länder

4.1.1 Nationella strategier

En slutsats som många länder dragit är att ett viktigt hjälpmedel för att lyckas med samordningen av informationssäkerhetsarbetet är att det finns en väl förankrad nationell strategi. Exempel på detta är att under de senaste åren har bl.a. USA, Storbritannien, Norge, Finland m.fl. tagit fram denna typ av övergripande styrdokument.

Strategidokument finns för flera nivåer och verksamheter. För utredningens vidkommande diskuteras några olika varianter. Den mest övergripande strategin är vad man skulle kunna kalla nationell och inbegriper både den privata och den offentliga sektorn. En del

strategier inriktar sig mot mer avgränsande områden så som t.ex. den statliga förvaltningen eller bara e-förvaltning.

I Finland fastslogs i september 2003 en strategi, vilken omfattar hela samhället och syftar till att stärka medborgarnas och företagens förtroende för informationssamhället genom bättre informationssäkerhet (i strategin används ordet datasäkerhet) och integritetsskydd. I den finländska strategin formuleras följande mål:

- främja nationellt och internationellt informationssäkerhetssamarbete
- främja den nationella konkurrenskraften och förutsättningarna för finländska företag i IT-branschen
- förbättra behärskande av informationssäkerhetsriskerna
- trygga de grundläggande rättigheterna och det nationella informationskapitalet
- utöka medvetenheten och kunskapen om informationssäkerhet

Den norska strategin från juni 2003 koncentrerar sig i sin tur på följande områden:

- skydda kritisk IT- infrastruktur
- samordning av regelverk för IT-säkerhet
- koordinering av arbetet med IT-säkerhet.
- genomförande av risk och sårbarhetsanalyser
- klassificering av information och informationssystem
- medvetandegöra alla aktörer
- varna och ge råd
- branschen och leverantörernas ansvar
- certifiering av kritiska system
- stärka kompetensen inom informationssäkerhetsområdet
- möjliggöra användandet av elektronisk signatur och PKI (Public Key Infrastructure)
- delta i internationellt samarbete

Syftet med den norska strategin är att:

- skapa en nationell helhetssyn på arbetet med IT-säkerhet
- reducera sårbarheten i teknisk infrastruktur
- skapa förutsättningar för ökad elektronisk samverkan

- etablera en enhetlig grund för politiska beslut och prioriteringar
- synliggöra behovet av koordinering av alla aspekter på IT-säkerhet

Finland och Norge är två exempel på länder som har nationella strategier. Den finska strategin omfattar hela samhället medan den norska i princip kan sägas inrikta sig på offentlig förvaltning. Till detta kommer att EU:s medlemsstater också samarbetar inom ramen för e-Europa. Se vidare i avsnittet om EU.

4.1.2 Övergripande organisationsfrågor

Flera länder har sedan länge civila myndigheter för informationssäkerhet, exempelvis Tyskland. I några länder, t.ex. Norge har sådana myndigheter skapats under senare år. I många fall finns det en koppling till signalspaningsorganisationer, då kunskapen om signalspaning också är väsentlig när man utformar skydd.

För utredningen är det intressant att se hur denna typ av myndigheter passar in i förvaltningsstrukturen. I Frankrike har frågorna placerats centralt i premiärministerns kansli, genom skapandet av Direction centrale de la sécurité des systèmes d'information (DCSSI) 2001. DCSSI ingår i Secrétariat Général de la Défense Nationale (SGDN) som sorterar direkt under premiärministern.

Även Tyskland har en informationssäkerhetsmyndighet Bundesamt für Sicherheit in der Informationstechnik (BSI) som sorterar under inrikesministeriet. Det är en civil myndighet som samlar flera viktiga informationssäkerhetsområden (se nedan).

I Storbritannien kan bilden sägas vara mer splittrad. I Cabinet Office,där tvärsektoriella frågor, eller andra frågor av särskild vikt samlas, finns Central Sponsor for Information Assurance (CSIA). Den IT-tekniskt inriktade organisationen Communications Electronics Security Group (CESG) lyder under utrikesdepartementet (Foreign and Commonwealth Office). National Infrastructure Security Co-ordniation Centre (NISCC) lyder under inrikesministeriet (Home Office).

Norge har inrättat en särskild informationssäkerhetsmyndighet, Nasjonal sikkerhetsmyndighet (NSM) under försvarsdepartementet. Myndigheten skall koordinera förebyggande säkerhet och kontrollera säkerheten inom sitt verksamhetsområde. Ett intressant organisatoriskt grepp är att myndigheten administrativt lyder under försvarsdepartementet och rapporterar dit vad avser militära frågor, men till justitiedepartementet när det gäller den civila sektorn.

4.1.3 Informationssäkerhetsarbetet i allmänhet

Direction centrale de la sécurité des systèmes d'information (DCSSI) som består av drygt 100 personer är den huvudsakliga organisationen för informationssäkerhetsfrågor i Frankrike. Mycket av den kvalificerade informationssäkerhetsverksamheten, som t.ex. kryptografi, finns också i organisationen. DCSSI är också certifieringsorgan och ansvarigt för det franska systemet för evaluering och certifiering av IT-säkerhet.

Den franske premiärministern uppmärksammade under hösten 2003 den otillfredsställande informationssäkerhetsnivån inom regeringen. Därför har en plan för att stärka informationssäkerheten tagits fram, vilken antogs vid utgången av 2003. Denna plan omfattar bl.a. organisationen centralt och lokalt, personalresursfrågor, industriella och tekniska aspekter av produkter och utveckling samt upphandling av utrustning.

Sedan 1991 finns Bundesamt für Sicherheit in der Informationstechnik (BSI) i Tyskland. BSI arbetar inom flera områden:

- strategiska tillämpningar (t.ex. e-förvaltning)
- Internetsäkerhet
- nätsäkerhet
- kryptologi
- forskning för IT-säkerhet
- skydd mot avlyssning
- allmän informationssäkerhet (grundstandarder)

BSI ger ut generella rekommendationer i samhället med målet att höja informationssäkerheten i allmänhet och speciellt för e-myndigheter och näringslivstillämpningar. BSI:s rekommendatio-

ner är inte bindande men andra civila myndigheter följer dem i hög utsträckning. BSI har även ansvaret för det nationella systemet för evaluering och certifiering av IT-säkerhet enligt IS 15408 och verkar även som certifieringsorgan. BSI bistår även med s.k. aktiv IT-kontroll (test av säkerheten genom angrepp av systemen under ordnande former).

I Norges Nasjonal sikkerhetsmyndighet har verksamheten organiserat sig i fyra olika avdelningar. Verksamheten beskrivs som:

- planer och analyser, säkerhetsanalyser, juridisk verksamhet och undervisning
- kryptosäkerhet, säkerhetsadministration och kontroll, kommunikationssäkerhet och fysik säkerhet samt informationssystemsäkerhet
- teknisk säkerhet, systemintegration, evaluering och certifiering och intrångstester
- personkontroll och personell säkerhet

Myndigheten är verksam sedan den 1 januari 2003 och har en personalstyrka på omkring 120 personer.

I Storbritannien är Central Sponsor for Information Assurance (CSIA) en del av Cabinet Office och har till uppgift att arbeta med frågor för hela förvaltningen. CSIA ansvarar för att det, i huvudsak, förebyggande arbetet för informationssäkerhet kommer tillstånd genom att:

- ge strategisk inriktning för informationssäkerhet för hela UK
- samordna och komplettera informationssäkerhetsarbetet
- stödja aktiviteter som utvecklar informationssäkerheten
- ackreditera system som används i hela förvaltningen
- identifiera och avhjälpa sårbarheter i de nationella telekommunikationerna.

Communications–Electronics Security Group (CESG) är den tekniska informationssäkerhetsgrenen i det brittiska systemet och ansvarar för alla tekniska aspekter i skyddet av offentlig användning av IT och kommunikationssystem. Inom ramen för detta arbete så hjälper CESG till med informationssäkerhetspolicy och riktlinjer. CESG ansvarar också för att stödja olika departement, myndighe-

ter, försvarsmakten och olika typer av tvärsektoriella program som e-myndigheter och nationella program för skydd mot datorintrång. Organisationen har skapat ett brittiskt system för evaluering och certifiering av IT-säkerhet och fungerar som certifieringsorgan för IT-säkerhet. CESG sorterar administrativt under den brittiska signalspanings- och tekniska organisationen Government Communications Headquarters (GCHQ).

4.1.4 Organisation av arbetet med kritisk infrastruktur

I Frankrike hanteras frågorna om kritisk infrastruktur i allt väsentligt av underrättelse- och säkerhetstjänsterna. Insynen i detta arbete är begränsat. I och med skapandet av DCSSI (se ovan) har frågorna dock fått en större tyngd och bredare innebörd.

Inom området skydd av samhällsviktig informationsinfrastruktur har den tyska staten beskrivit sin målsättning som en strävan efter att skapa förtroende och samarbete mellan aktörer inom det s.k. CIIP-nätverket. Staten skall ta ett ansvar för kritisk information och säkra att skydd av samhällsviktig informationsinfrastruktur är en nationell uppgift. I detta sammanhang bidrar BSI med intersektoriella aspekter. De viktigaste departementen med ansvar för kritisk infrastruktur på förbundsnivå i Tyskland är inrikesdepartementet (Bundesministerium des Innern), näringsdepartementet (Bundesministerium für Wirtschaft und Arbeit), och försvarsministeriet (Bundesministerium der Verteidigung). Dessa stöds av den tyska informationssäkerhetsmydigheten, Bundesamt für Sicherheit in der Informationstechnik (BSI) som lyder under inrikesdepartementet. Andra aktörer inom den federala administrationen är den brottsbekämpande myndigheten Bundeskriminalamt (BKA). Den federala underrättelsetjänsten, Bundesnachrichtendienst (BND), är ansvarig för att sammanställa hotanalyser.

I Storbritannien är det National Infrastructure Security Coordination Centre (NISCC) som sedan 1999 har till uppgift att samordnat skydda den kritiska infrastrukturen mot elektroniska attacker, dvs. inte misstag, olyckor eller andra oavsiktliga hot. Samordningen gäller:

- arbetet med att identifiera och höja säkerheten för kritiska system

- information och varningar om attacker
- stöd vid allvarliga attacker
- information om hot
- specialistråd och expertis inom informationssäkerhet

NISCC arbetar med partnerskap och är inte en reglerande myndighet. I praktiken är NISCC ett samverkansorgan inom vilket flera myndigheter samarbetar. En stor del av resurserna kommer från British Security Service (BSS, historiskt mer känt som MI5). CESG bidrar med teknisk kompetens. Den militära Joint Systems Coordination Centre (JsyCC) är också med. Organisationen leds av en styrelse bestående av representanter från de ingående organisationerna och flera departement samt polisen. Vad gäller telekommunikationer har den tidigare nämnda Central Sponsor for Information Assurance till uppgift att identifiera och avhjälpa sårbarheter i de nationella systemen.

En annan intressant verksamhet är det norska försöket i Nasjonal sikkerhetsmyndighet (NSM) med övervakning av kritiska informationsinfrastrukturer och det s.k. Senter for informasjonssikring (SIS). En av SIS huvuduppgifter är att samordna aktiviteter kring IT-säkerhet i Norge och skapa en helhetsbild av hoten mot IT-system. För detta ändamål har SIS ingen direktivrätt utan skall bygga upp informationskanaler på förtroendeskapande basis. En av de viktigaste informationsskällorna är det s.k. Varslingssystem for Digital Infrastruktur (VDI). Det består av sammankopplade intrångsdetekteringssystem mellan Politiets sikkerhetstjeneste (PST), Forsvarets etterretningstjeneste (FO/E) och ett antal företag och myndigheter. Projektet har varit en framgång och blivit en permanent funktion inom Nasjonal sikkerhetsmyndighet.

4.1.5 Lagstiftning

En annan utveckling under de senaste åren är att flera länder har ändrat sin lagstiftning i syfte att skydda den informationstekniska infrastrukturen. En av de drivande krafterna bakom detta arbete har varit behovet av att skydda den kritiska informationsinfrastrukturen från obehörig användning, vilket gäller allt från dataintrång till terrorism. Lagstiftningen ger med varierande begränsningar, till skydd för den personliga integriteten, möjlighet till bevakning av elektronisk kommunikation i syfte att skydda kritisk infrastruktur.

Detta gäller t.ex. andra europeiska länder som Danmark, Norge, Nederländerna, Storbritannien och Tyskland. I vilken omfattning det praktiska arbetet sker är inte alltid möjligt att följa i och med att detta till viss del sker under sekretess.

4.1.6 Rättsvårdande åtgärder

Som redogörs närmare för i avsnitt 6 så krävs i många fall särskild kompetens för utredning av brott med anknytning till informationsteknik. Detta har lett till inrättandet av specialiserade funktioner inom polisorganisationerna i många länder, där man samlat personer med nödvändiga kunskaper för utredning av IT-relaterad brottslighet.

Ett exempel på detta finns i Storbritannien, där National Hi-Tech Crime Unit (NHTCU) sedan november 2000 arbetar för att bekämpa IT-relaterad brottslighet av nationell eller transnationell karaktär. En viktig komponent i NHTCU:s arbete är samverkan med andra sektorer. Bland annat ingår NHTCU som ordförande i ett inrättat forum för IT-brottslighet, där Internetleverantörer, polisen och näringslivet ingår, och man är också en del av NISCC:s nätverk.

Experter från de nationella IT-brottsrotlarna samlas på det internationella planet bl.a. i Interpols Working Party on Information Technology Crime. Gruppens europeiska förgrening (EWPITC) har bl.a. tagit fram en manual för utredning av IT-relaterad brottslighet och ordnar även kurser flera gånger per år. Vartannat år arrangeras även en storkonferens för samtliga medlemsländer, då en del av konferensen även är öppen för näringslivet. Bland andra initiativ på den internationella arenan märks G8:s nätverk för högteknologisk brottslighet med kontaktpunkter inte bara i länderna som deltar i G8-samarbetet utan även i ett stort antal andra länder.

4.1.7 Samarbete mellan privat och offentlig sektor

Både inom det generella arbetet med informationssäkerhet och vad avser skyddet av kritisk infrastruktur finns ett brett erkännande av att det är nödvändigt att samarbeta med näringslivet.

I Tyskland har olika slag av koordineringsaktiviteter mellan offentlig sektor och näringsliv under de senaste åren genomförts. Det finns ett flertal samverkansinitiativ mellan offentlig och privat sektor med relevans för kritisk infrastruktur. Även egna initiativ inom näringslivet förekommer.

I Schweiz finns sedan 1999 stiftelsen InfoSurance som samlar privat och offentlig sektor för att öka medvetenheten om informationssäkerhet bl.a. genom förebyggande arbete.

I USA finns inom den privata sektorn branschvisa Information Sharing and Analyses Center (ISAC). Dessa centrum har informella relationer med Department of Homeland Security (DHS). Federal Bureau of Investigation (FBI) och dess division för Cybersecurity har hand om det s.k. Infragard-programmet. Programmet innebär en form av informationsutbyte på lokal nivå mellan FBI, polis och näringsliv.

4.1.8 Utbildningsfrågor

Många länder satsar också på utbildning inom informationssäkerhetsområdet, vilket både sker på bredden (t.ex. information om hot och risker) och på djupet (t.ex. kvalificerade informationssäkerhetsutbildningar på flera år). I detta sammanhang kan det vara intressant att notera att den ovan nämnda franska planen också tar upp personalresursfrågor inklusive utbildning.

I Storbritannien har utbildningsfrågorna belysts på flera nivåer. För staten och dess egna system avses utbildningen för de som utvecklar, ackrediterar och sköter driften av system att stärkas – en tydligare professionalisering av informationssäkerhetsyrket. Samtidigt avses utbildningssektorn påverkas till att inkludera informationssäkerhetsfrågorna på universitets- och högskolenivå. Problemet med barn och ungdomar som hackar datorer gör också att frågor om användningen av datorer kanske behöver tas upp i skolor.

4.1.9 IT-incidenthantering

Allt fler länder och organisationer satsar också på olika typer av CERT-funktioner (Computer Emergency Response Team), dvs.

grupper som har specialiserat sig på IT-incidenthantering. (En annan vanligare benämning är CSIRT (Computer Security Incident Response Team).

Syftet med en CSIRT är att ge förebyggande råd och stöd samt minska riskerna för att drabbas av en IT-säkerhetsincident. Den kan ofta också ge stöd vid pågående incidenter och för att återställa systemen efter en incident. IT-incidenthanteringsgrupper finns inom statsförvaltningar och allt oftare inom företag.

I Finland sker IT-incidenthanteringen inom den CERT-FI som är en enhet för informationssäkerhet vid Kommunikationsverket. Kommunikationsverket har hand om CERT-arbetsgruppen, som är ett samarbetsorgan för olika operatörer och som arbetar med upptäckt och utredning av informationssäkerhetskränkningar.

I Norge ligger CERT-funktionen inom den nybildade Nasjonal Sikkerhetsmyndighet (NSM).

I Frankrike är det tidigare nämnda Sécretariat Géneral de la Défence Nationale (SGDN) de som ansvarar för statsförvaltningens CERT-liknande funktion.

I Storbritannien finns sedan lång tid UNIRAS (Unified Incident Reporting and Alert Scheme) som började som en CSIRT för förvaltningen. En intressant brittisk utveckling är de s.k. WARP (Warning, Advice and Reporting Points), vilket är en enkel variant av en CSIRT. En WARP kan betjäna små och medelstora företag, organisationer eller grupper av medborgare.

I Tyskland driver BSI en CSIRT för i första hand statsförvaltningen men också för den privata sektorn. Den tyska IT-incidenthanteringsgruppen arbetar både förebyggande och hjälper till när en IT-säkerhetsincident har inträffat. I Tyskland finns också CERT-Verbund som organiserar flera tyska CSIRT:ar, från forskningsnät, Siemens, Deutsche Telekom, banker m.fl.

I Nederländerna driver den nederländska organisationen för IT i den offentliga sektorn (ICTU), på uppdrag av inrikesdepartementet, en CERT-funktion för statsförvaltningen (GOVCERT.NL).

Under år 2002 etablerade ett antal europeiska länder med statliga CERT-organisationer ett aktivt samarbete på operativ nivå – European Government CERT Group (EGC). I EGC ingår Storbritannien, Tyskland, Frankrike, Nederländerna, Finland och Sverige.

CERT Coordination Center (CERT/CC) är ett federalt finansierat forsknings- och utvecklingscenter vid Carnegie Mellon University. CERT/CC tillkom redan 1988 efter att den s.k. Morrismasken drabbat 10 % av Internet. Som ett samarbetsprojekt mellan CERT/CC och Department of Homeland Security har det nystartade US-CERT nyligen tagit över ansvaret för CERT-funktionen efter tidigare FedCIRC, som sorterade under General Services Administration. Avsikten är att US-CERT efterhand också skall samarbeta med den privata sektorn och andra nationella och internationella organisationer.

I Australien är AusCERT en oberoende, idéell organisation vid det fristående University of Queensland. Den australiensiska regeringen betalar en del av dess kostnader. AusCERT spelar en intressant roll. Många datavirus sprids när användare kommer till sina arbetsplatser och börjar använda sina datorer. Aus-CERT:s samarbete med andra grupper blir då viktigt eftersom Australien, i tidszoner mätt, ligger före länder med hög IT-användning i Europa och Nordamerika. AusCERT har alltså möjlighet att skicka ut varningar innan arbetsdagen har börjat t.ex. i Sverige.

De engelskspråkiga ländernas CERT-funktioner har sedan länge ett nära samarbete exempelvis vad gäller utbyte av operativ varningsinformation.

4.1.10 Information till allmänheten

Generellt kan utredningen notera att offentliga myndigheter i många länder sprider information till allmänheten med råd om vad som krävs för att uppnå högre säkerhet vid nyttjandet av informationsteknik.

Exempel på detta är att Bundesamt für Sicherheit in der Informationstechnik (BSI) har ett tydligt slutanvändarfokus inom bl.a. Internetsäkerhet - information finns tillgänglig på en webbplats och

man skriver artiklar i datortidningar. BSI har också låtit distribuera en cd med information och program riktad till hushåll.

I Nederländerna har man en kampanj om säker användning av Internet. Ett intressant inslag har varit att man tillsammans med en serietidning producerat en specialtidning om säkerhet riktad till barn. I Belgien finns ett datavirusvarningssystem som vid allvarliga incidenter kan gå ut via radio och varna allmänheten.

Ett ovanligare exempel är ett inslag i den finländska strategin, den nationella dagen för informationssäkerhet, som arrangerades för första gången 11/2 2004 (jfr nödnumret 112) i Finland. Målet med dagen är att alla datorer anslutna till Internet skall förses med uppdaterat operativsystem, brandvägg och datavirusbekämpningsprogram som uppdateras tillräckligt ofta. Över en miljon finländska hushåll fick en informationssäkerhetsguide med sin morgontidning.

4.1.11 Utredningens iakttagelser

En slutsats som flera länder dragit är att en nationell strategi underlättar arbetet med att samordna informationssäkerhetsarbetet. Informationssäkerhetsarbetet, i bred bemärkelse, i ett land innehåller flera områden som kräver särskild kunskap. Det kan röra sig om allt från grundläggande tekniska frågor om IT-system, kommunikationssäkerhet, administrativa stöd och regler, till frågor om styrning och reglering på en övergripande nivå i samhället.

I flera länder har informationssäkerheten i kritisk infrastruktur fått särskild uppmärksamhet. I många infrastruktursystem spelar de stödjande IT-systemen ibland en helt avgörande roll för att kärnverksamheten skall fungera. Inom detta område ser flera länder att det är en statlig angelägenhet att system är säkra, samtidigt är det en utmaning att ordna samarbetet och kraven på de ofta privata ägarna av systemen.

Ett annat område som är lätt att urskilja i informationssäkerhetsarbetet är statens egna system. Flera länder har organisationer som arbetar för att bygga upp och följa upp säkerheten i dessa system.

Det är också tydligt att polisiära, militära och underrättelseorgan är organisationer som utför specifikt arbete eller har behov av expertkompetens inom sina områden. Informationssäkerhetskompetensen är inte bara till för att garantera säkerheten i de egna systemen utan kan också användas för t.ex. tekniska undersökningar av utrustning som används vid brott eller för att underlätta underrättelseinhämtning.

Ett annat område som också har uppmärksammats är att för hemanvändarnas och små och medelstora företags behov, står ofta användningen av Internet i fokus. I vissa fall lyfts även sekundära frågor fram. Bristande informationssäkerhet kan leda till att en organisation tappar allmänhetens eller kundernas förtroende om information kommer i fel händer.

Flera länder har en sammanhållen struktur för informationssäkerhetsarbetet, t.ex. inom en myndighet. En fördel med detta är att de kan vara en tillgång i det internationella samarbetet.

Den som ger råd i förebyggande informationssäkerhetsarbete och vid incidenter måste ha hög kompetens och god kännedom om flera områden som berör informationssäkerhet, t.ex. rörande hur systemen är uppbyggda (operativsystem och nät), skydd mot intrång (brandväggar och skydd mot datavirus), samt skydd mot avlyssning (röjande signaler och kryptografi).

Området innehåller kunskap som om den kommer i fel händer kan innebära nya säkerhetsrisker. Det kan t.ex. gälla hur krypton kan forceras eller kunskap om nya säkerhetsbrister innan det finns uppdateringar. Ofta är det nödvändigt att behärska flera av dessa kompetensområden för att kunna lösa informationssäkerhetsproblem.

De olika sätten att organisera arbetet som utredningen har tagit del av har alla berört samordningen och samlande av kunskap inom informationssäkerhetsarbetet.

En annan organisatorisk utmaning som utredningen har noterat är att, utöver det vardagliga säkerhetsarbetet, kunna ta del av information om hot eller avancerade skyddstekniker som hittills har funnits i polisiära eller underrättelseorganisationer. Särskilt gäller detta kritisk infrastruktur. Detta måste kunna ske utan att känslig infor-

mation röjs. Samtidigt behövs en öppen hållning för att lämna ut information och råd och även uppmuntra till samarbete. Närliggande frågor är också utveckling och evaluering av IT-säkerhetsprodukter.

4.2 Lägesbeskrivning av internationellt arbete med informationssäkerhetsfrågor

4.2.1 Europeiska unionen (EU)

Från utredningens horisont finns det flera anledningar att bevaka informationssäkerhetsfrågorna inom EU. Inom unionen pågår ett harmoniseringsarbete där medlemsländerna närmar sig varandra både vad gäller lagstiftning och definitioner inom informationssäkerhetsområdet. Förutom denna tillnärmning av medlemsstaternas lagstiftning, som sker främst i medlemsstaternas intresse, så har unionen, eftersom den är en organisation som hanterar sekretessbelagd information, ett intresse av att skydda sin egen information. För att arbetet inom unionen skall kunna utvecklas även på områden som kräver sekretess har det varit nödvändigt för unionen att anta säkerhetsbestämmelser med regler om hantering av sekretessbelagda EU-uppgifter.

Harmoniseringsarbete inom unionen

Sedan 1990-talet finns ett antal direktiv, meddelanden och förslag som berör informationssäkerheten. En milstolpe i detta arbete och startskottet för en mer samlad ansats på informationsteknikens område var EU:s toppmöte i Lissabon i mars 2000, då EU:s stats- och regeringschefer enades om ett nytt strategiskt mål för unionen, den s.k. Lissabonstrategin. Strategin innebär bl.a. att Europa inom tio år skall bli den mest konkurrenskraftiga och dynamiska kunskapsbaserade ekonomin.

Vid Europeiska rådets möte i Feira i juni 2000 fastställdes handlingsplanen e-Europa 2002 Ett informationssamhälle för alla som sedan efterträtts av e-Europa 2005 (eEurope används i EU-dokument). Dessa båda planer ingår som led i genomförandet av Lissabonstrategin. Ett av målen med den första handlingsplanen var

att åstadkomma ett billigare, snabbare och säkrare Internet. Syftet med handlingsplanen e-Europa 2005 är att skapa en miljö som är gynnsam för privata investeringar och skapandet av nya arbetstillfällen, att öka produktiviteten, att modernisera de offentliga tjänsterna och att ge alla möjlighet att delta i det globala informationssamhället. Därför syftar e-Europa 2005 till att få fram säkra tjänster och tillämpningar och innehåll som bygger på lättillgänglig bredbandsinfrastruktur.

EU:s engagemang i informationssäkerhetsfrågorna har bl.a. haft sin utgångspunkt i främjande av handeln. e-Europa 2005 bygger på två olika åtgärder som ömsesidigt stärker varandra; dels stimulera utvecklingen av tjänster, tillämpningar och innehåll, dels hantera frågor som rör den underliggande bredbandsinfrastrukturen och säkerheten. De två är en övergripande policy, som rymmer och har kopplingar till, åtgärder inom många verksamhetsområden, både inom ramen för EU:s första pelare och dess tredje pelare.

Från utredningens horisont är arbetet inom EU intressant även för de intryck och den inspiration som unionens egna säkerhetsarbete kan ge. Unionen har i Rådets säkerhetsbestämmelser (EG 264/2001) skapat ett säkerhetssystem som skall bidra till att utveckla rådets verksamhet på områden som kräver olika grader av sekretess.

EU:s första pelare

Europeiska rådet erkände vid sitt möte i Stockholm i mars 2001 behovet av ytterligare insatser i fråga om nät- och informationssäkerhet och uppdrog åt rådet tillsammans med kommissionen att utarbeta en övergripande strategi för säkerheten när det gäller elektroniska nät tillsammans med praktiska åtgärder för dess genomförande. Som svar på detta presenterade kommissionen i juni samma år ett meddelande Nät- och informationssäkerhet: förslag till en europeisk strategi. I meddelandet analyseras aktuella problem rörande nätsäkerhet och där ges även en strategisk plan för åtgärder inom detta område. I meddelandet konstateras även att åtgärder för nät- och informationssäkerhet måste sättas in i en kontext och ses i ett sammanhang med telekommunikationer, dataskydd och IT-relaterad brottslighet. Som definition av begreppet nät- och informationssäkerhet anges förmågan hos ett nät att tåla, vid en viss till-

förlitlighetsnivå, 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.

Som förslag på åtgärder för att förbättra nät- och informationssäkerheten föreslås i kommissionens meddelande medvetandehöjande åtgärder, förbättrad CERT-funktion och samordning inom Europa, stöd till forskning, stöd för marknadsorienterad standardisering och certifiering, lagstiftning mot IT-relaterad brottslighet, säkerhet i myndigheters system, internationellt samarbete.

Meddelandet följdes i rådet upp av en rad resolutioner. Den första antogs i december 2001 och rörde en gemensam inställning och särskilda åtgärder på området för nät- och informationssäkerhet. I januari 2002 antogs ytterligare en resolution av rådet där medlemsstaterna bl.a. uppmanas att arbeta för ökad medvetenhet när det gäller nät- och informationssäkerhet, se över effektiviteten hos nationella arrangemang för hanteringen av IT-incidenter samt främja användandet av standarden Common Criteria. Rådet antog även i februari 2003 en resolution om en säkerhetskultur som med hänvisning till OECD:s riktlinjer betonar internationellt samarbete, öppenhet, informationsutbyte mellan EU-institutioner, medlemsstaterna och den privata sektorn.

En viktig utveckling på informationssäkerhetens område inom unionen är inrättandet av den europeiska nät- och informationssäkerhetsbyrån (Enisa). Förordningen om byrån förväntas träda i kraft under våren 2004. Byrån skall bedriva verksamhet under fem år. Beroende på antalet nya medlemsstater får byrån 31-44 anställda och en budget på 24,3-33,3 miljoner euro för hela perioden.

Byrån skall främja gemenskapens, medlemsstaternas, och som en följd av detta, näringslivets förmåga att förhindra, ta itu med och lösa problem som rör nät- och informationssäkerhet. Byrån skall ge stöd och råd åt kommissionen och medlemsstaterna i frågor som rör nät- och informationssäkerhet.

Genom att utveckla sakkunskap, baserad på medlemsstaternas och gemenskapens tidigare arbete skall byrån främja ett brett samarbete mellan privat och offentlig sektor. På begäran skall byrån även

stödja kommissionen i det tekniska föreberedelsearbetet för uppdatering och utveckling av gemenskapslagstiftningen inom området.

Utöver att ge råd till kommissionen, Europaparlamentet och medlemsstaterna skall byrån bl.a.:

- analysera framväxande risker, framför allt på europeisk nivå
- bidra till större medvetenhet om nät- och informationssäkerhet
- förbättra samarbetet mellan och inom t.ex. näringslivet, forskare, leverantörer och användare av produkter och tjänster inom området
- möjliggöra samarbete om utveckling av metoder för att förebygga och hantera informationssäkerhetsproblem
- bidra till det internationella samarbetet.

Beträffande finansiering av åtgärder inom informationssäkerhetens område öppnar EU för några möjligheter. EG:s 6:e ramprogram för forskning är gemenskapens finansieringsinstrument för att stärka den europeiska industrins konkurrenskraft och omsätta initiativet Ett europeiskt forskningsområde i praktisk verklighet. Ansvaret för genomförande av ramprogrammet ligger på kommissionen och det genomförs tillsammans med medlemsstaterna via programkommittéer. Inom ramprogrammet finns ett ämnesområde som kallas Informationssamhällets teknik. Detta delområde har för perioden fram till och med 2006 tilldelats 3,625 miljarder euro. Inom detta område kan forsknings- och utvecklingsprojekt stödjas som stödjer industrins konkurrenskraft, men också bidrar till genomförandet av handlingsplanen för e-Europa.

Ett annat initiativ som också syftar till att komplettera de nationella insatserna för att omvandla Europa till en kunskapsbaserad ekonomi är det finansiella stödprogrammet (Modinis). Tanken är att resurser skall sättas av för att övervaka och stödja medlemsstaternas insatser för att genomföra handlingsplanen e-Europa 2005. Medlen skall även kunna användas till att analysera de ekonomiska och samhälleliga följderna av informationssamhället och att stärka de nationella och europeiska insatserna för att förbättra nät- och informationssäkerheten.

För att uppnå dessa mål har det beslutats att inom ramen för programmet bl.a. finansiera åtgärder så som riktmärkning (benchmar-

king) och utbyte av s.k. bästa förfaranden (best practices) i Europa. Programmet skall även bidra till finansiering av förberedelser inför inrättandet av den europeiska nätverks- och informationssäkerhetsbyrån (Enisa), bl.a. genom att finansiera undersökningar, studier och workshops rörande informations- och nätsäkerhet. Programmet kommer att löpa i tre år (2003–2005) med en budget på 21 miljoner euro. Detta program ersätter det tidigare Promiseprogrammet som också finansierade liknande åtgärder.

EU:s andra pelare

EU driver inom ramen för den gemensamma utrikes- och säkerhetspolitiken frågor som rör krishantering med bl.a. militära resurser. EU:s militära stab (EUMS) har uppgiften att utveckla EU:s militära förmåga till krishantering. För att samordna de olika medlemsländernas syn på lösandet av uppgiften, skapar EUMS tillsammans med deltagare från respektive lands militära organisationer ett antal militära koncept. Varje lands politiska nivå godkänner därefter arbetet med denna målsättning.

Vad avser EU och informationsoperationer är konceptet för informationsoperationer godkänt av alla medlemsländer. Konceptet vilar på EU:s övergripande informationsstrategi, vilket är ett strategiskt styrdokument för hur EU avser att använda information i en krishanteringssituation. Informationsoperationer bedöms vara en resurs för att minska behovet av direkta vapeninsatser. I konceptet markeras tydligt vikten av att nationella och internationella lagar och förordningar respekteras. De olika elementen inom informationsoperationer består enligt EU-konceptet av fysisk bekämpning, elektronisk krigföring, vilseledning, operationssekretess, psykologiska operationer, civil-militär samverkan och dator- och nätverksattacker.[10]

[10] Definitionen av militära informationsoperationer som antagits av EU: ”EU Mil Info Ops are all co-ordinated actions undertaken to influence parties to the crisis and other audiences, in support of political and military objectives of the EU, through affecting their information, information based process and systems and their decision makers. These actions can be defensive or offensive according to their objective.”

EU:s tredje pelare

Europeiska rådets möte i Tammerfors i oktober 1999 ägnades åt diskussioner kring skapandet av en union byggd på frihet, säkerhet och rättvisa. Inom ramen för åtgärder för att motverka den organiserade brottsligheten omnämndes även högteknologisk brottslighet som en brottstyp som bör omfattas av insatser för att enas om gemensamma definitioner, grunder för åtal och påföljder. Detta återfanns sedan i handlingsplanen för e-Europa 2002 där ett av målen sades vara bättre samordning i kampen mot IT-brottslighet. Som ett led i sin insats att bekämpa IT-brottsligheten presenterade kommissionen i januari 2001 sitt meddelande Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet. Meddelandet behandlade möjliga former för ett allomfattande politiskt initiativ inom ramen för de mer allmänna målen i informationssamhället och frihet, säkerhet och rättvisa för att förbättra säkerheten i informationsstrukturerna och bekämpa den IT-relaterade brottsligheten. En av kärnfrågorna i meddelandet var behovet av effektiva åtgärder för att motverka hoten mot informationssystemens och datanätens autencitet, integritet, konfidentialitet och tillförlitlighet. Kommissionen identifierade ett behov av gemensam EU-lagstiftning rörande bl.a. tillnärmning av medlemsstaternas lagstiftning avseende barnpornografi och brott mot systemintegritet (t. ex. hackning), ömsesidigt erkännande av rättsliga beslut (t. ex. beslagsbeslut) samt utvärdering av behov av ett särskilt initiativ om trafikdata. Vidare föreslog kommissionen inrättande av ett EU-forum mot IT-brottslighet.

I juni samma år presenterades även det ovan omnämnda meddelandet med förslag till en europeisk strategi för nät- och informationssäkerhet. I det redovisar kommissionen vad man avser med attacker mot informationssystem:

- olaga intrång i informationssystem
- störningar av informationssystem
- körning av destruktiva program som modifierar eller förstör data
- uppsnappande av kommunikation
- vilseledande framställning av data

För att möta dessa hot, men även för att bidra till åtgärderna att möta hotet om terroristangrepp mot vitala informationssystem i EU, påbörjades våren 2002 förhandlingar om ett rambeslut om angrepp mot informationssystem. Rambeslutet tillsammans med den europeiska arresteringsordern (EGT L 190, 18/7/2002) och rambeslutet om bekämpande av terrorism (EGT L 164, 22/6/2002) innebär enligt kommissionen att EU får en effektiv strafflagstiftning för att möta cyberterrorism och ett förbättrat internationellt samarbete mot terrorism.

Rambeslutet om angrepp mot informationssystem kompletterar vad som redan uppnåtts i form av gemenskapslagstiftning om skydd av informationssystem. I synnerhet EU-ramlagstiftningen om telekommunikationer och uppgiftsskydd (direktiv 95/46/EG och 97/66/EG) innehåller bestämmelser som syftar till att leverantörer av allmänt tillgängliga telekommunikationstjänster skall vidta de tekniska och organisatoriska åtgärder som behövs för att deras tjänster skall uppfylla krav på säkerhet och konfidentialitet, och att dessa åtgärder bidrar till en tillräcklig säkerhetsnivå med avseende på de aktuella riskerna.

Enligt kommissionen innehåller medlemsstaternas lagstiftning på detta område vissa betydande luckor och skillnader som kan vara till hinder i kampen mot organiserad brottslighet och terrorism och mot angrepp mot informationssystem som utförs av individer. En tillnärmning av de straffrättsliga bestämmelserna om högteknologisk brottslighet syftar till att den nationella lagstiftningen skall vara så enhetlig att det går att utreda alla allvarliga angrepp med hjälp av den teknik och de metoder som straffrätten medger. Förövarna av dessa brott måste identifieras och ställas inför rätta, och domstolarna behöver ha lämpliga och proportionerliga påföljder till sitt förfogande. Sammantaget skulle detta sända starkt avskräckande signaler till dem som överväger angrepp mot informationssystem. En tillnärmning av lagstiftningen i medlemsstaterna underlättar även vid internationellt samarbete, genom att säkerställa att kravet på dubbel straffbarhet är uppfyllt, vilket är en viktig förbättring vid brott som liksom angrepp mot informationssystem inte sällan är av gränsöverskridande natur.

Rambeslutet om angrepp mot informationssystem har till syfte att tillnärma strafflagstiftningen när det gäller angrepp mot informationssystem samt att säkra största möjliga grad av polisiärt och

rättsligt samarbete när det gäller att bekämpa brott i samband med angrepp mot informationssystem. Rambeslutet innehåller bestämmelser om att uppsåtliga och orättmätiga intrång i (hackning) och störningar av (datavirus, tillgänglighetsattacker) informationssystem och datorbehandlade uppgifter skall vara straffbara. Begreppet ”Informationssystem” används i dess vidaste bemärkelse. Således omfattas t.ex. fickdatorer, mobiltelefoner liksom nätverk, servrar m.m. och Internet-infrastruktur.

Störningen kan rikta sig mot informationssystemet självt eller mot innehållet, genom att detta ändras eller raderas. Därutöver innehåller förslaget regler om medverkan och försök, påföljder och försvårande omständigheter, samt ansvar och påföljder för juridiska personer. Politisk enighet om rambeslutet nåddes vid justitieministermötet i februari 2003 och det är för närvarande föremål för genomförande i Sverige, tillsammans med Europarådets IT-brottskonvention. Kommissionen har i olika sammanhang beskrivit vikten av att skapa ett säkert informationssamhälle och sedan Amsterdamfördraget trädde i kraft har ett av unionens mål varit att göra unionen till ett område med frihet, säkerhet och rättvisa.

Under det svenska ordförandeskapet i EU beslutades efter förslag från Sverige att EU-länderna skulle ansluta sig till G8-arrangemanget med dyngnetruntservice istället för att skapa en egen liknande funktion inom EU. Det finns också ett förslag från G8 till Interpol att slå samman Interpols National Central Reference Point-arrangemang (NCRP) med G8-arrangemanget. Denna fråga bereds för närvarande inom Interpol.

Rådets säkerhetsbestämmelser (EG 264/2001)

Den 19 mars 2001 fattade Europeiska unionens råd beslut om säkerhetsbestämmelser, som 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). Det skall också 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, oavsett om upphovet till uppgifterna finns inom EU eller har erhållits från en medlemsstat, tredje land eller internationella organisationer. Med ”handlingar” avses ett antal fysiska medier (brev, rapporter etc.) och med ”materiel” avses alla handlingar samt varje slags utrustning eller vapen.

I bestämmelserna beskrivs grunderna för ”god säkerhet”. Till dessa grunder räknas en nationell säkerhetsorganisation för insamling och registrering av underrättelser om spionerі, sabotage, terrorism och annan omstörtande verksamhet. Säkerhetsorganisationen förutsätts även ge information och råd till regeringen (och genom denna till rådet) om arten av hotet och vilka skyddsåtgärder som kan vidtas.

Vidare förutsätts att varje medlemsstat har en teknisk myndighet för informationssäkerhet som är ansvarig för att tillsammans med den berörda säkerhetsmyndigheten tillhandahålla information och ge råd om tekniska hot mot säkerheten och vilka skyddsåtgärder som kan vidtas.

Slutligen förutsätts regelbundet samarbete mellan departement, myndigheter och berörda inom generalsekretariatet för att i tillämpliga fall fastställa och rekommendera vilka uppgifter, resurser och anläggningar som skall skyddas och vilka gemensamma skyddsnormer som skall gälla. Bestämmelserna skall enligt beslutet genomföras i medlemsstaterna och tillämpas på hantering av alla sekretessbelagda EU-uppgifter, som preciseras i beslutet.

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. Sårbarhet (vulnerability) kan definieras som en svaghet i kontrollerna eller en avsaknad av kontroller som kan underlätta eller möjliggöra att ett hot sätts i verket mot en specifik tillgång eller ett specifikt mål. Sårbarheten kan vara en försummelse eller höra samman med brister i en kontrolls verkningsfullhet (strength), fullständighet (completeness) eller konsekvens (consistency); den kan vara av teknisk (technical), förfarandemässig (procedural), eller operativ (operational) art.

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 särskilda 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.

Det kommer att krävas åtgärder för datasäkerhet (computer security) med vilket avses säkerhetsegenskaper för datorutrustning och programvara, för att genomföra principen om att endast den som har behov av vissa uppgifter för sin tjänsteutövning skall få tillgång till desamma. Åtgärderna krävs även för att kunna förhindra eller upptäcka obehörigt röjande av uppgifter. När säkerhetskraven fastställs skall det avgöras hur tillförlitliga åtgärderna för datasäkerhet är. Ackrediteringsförfarande skall avgöra att säkerhetsnivån är till-

räckligt hög för att man skall kunna lita på åtgärderna för datasäkerhet.

Säkerhetsbestämmelserna slår fast att det för alla system som hanterar EU-uppgifter med sekretessgraderna CONFIDENTIAL UE och högre skall krävas att en redovisning av systemspecifika säkerhetskrav (System-Specific Requirement Statement, SSRS) utarbetas av myndigheten för driften av IT-system (ITSOA), vid behov med indata och bistånd från projektpersonalen och myndigheten för informationssäkerhet, liksom att godkännas av ackrediteringsmyndigheten för säkerhet. Motsvarande procedur förutsätts för RESTRICTED-nivån.

Alla system som hanterar EU-uppgifter med sekretessgraden CONFIDENTIAL UE och högre skall ackrediteras för drift i former motsvarande dedikerad, högnivå, respektive flernivå.

Säkerhetspolisen har i en skrivelse den 30 november 2001 till regeringen anfört att enligt Säkerhetspolisens mening omfattas inte samtliga uppgifter som utgör sekretessbelagda EU-uppgifter av säkerhetsskyddslagens regler. Säkerhetspolisen har föreslagit att begreppet säkerhetsskydd skall utvidgas till att omfatta sekretessbelagda uppgifter som Sverige genom åtagande mot annan stat eller mellanfolklig organisation förbundigt sig att skydda. Frågan är föremål för beredning och en departementspromemoria där bl.a. denna fråga behandlas kommer att remitteras under mars månad 2004.

Sammanfattningsvis kan konstateras att initiativ på informationssäkerhetsområdet inom såväl första som tredje pelaren har sin bas i e-Europa, via kommissionens två meddelanden. Skillnader mellan IT-brottsmeddelandet och nätsäkerhetsmeddelandet är att det senare tar ett bredare grepp och ser till samtliga hot som nät kan utsättas för, såväl illvilliga (brottsliga) som oavsiktliga (beroende på okunskap eller slarv). Viktigt att komma ihåg är att det arbete unionen genomför för främjandet av informationssäkerhet har andra primära mål. Inom första pelaren har initiativen till lagstiftning till syfte att bidra till förverkligandet av den inre marknaden. Handeln sker i allt större utsträckning över Internet, vilket kräver en hög grad av säkerhet för att inte konsumenterna skall tappa förtroendet och denna form av handel stagnera. Detsamma gäller även andra former av elektroniska tjänster. På tredjepelarområdet är det för-

verkligandet av unionen som ett samhälle med frihet, säkerhet och rättvisa som utgjort grunden för initiativ om tillnärmning av lagstiftning på straffrättens område.

Oaktat detta har mycket skett inom ramen för EU-samarbetet, och den samsyn som skapas medlemsstaterna emellan i dessa frågor ger även effekter i andra internationella fora. Behandlingen av informationssäkerhetsfrågor inom EU har även aktualiserat frågan om gemensamma definitioner på området, kanske särskilt på straffrättens område men även unionens egna säkerhetsföreskrifter har ställt definitionsfrågan på sin spets. Redan vid Europeiska rådets möte i Tammerfors hösten 1999 togs högteknologisk brottslighet upp i en begränsad förteckning över områden där man bör eftersträva gemensamma definitioner, brottsbeskrivningar och påföljder.

4.2.2 Organisation for Economic Co-operation and Development (OECD)

I sitt arbete skall utredaren beakta OECD:s (Organisation for Economic Co-operation and Development) riktlinjer för nät- och informationssäkerhet och lämna förslag till hur riktlinjerna kan genomföras i utredarens förslag.

Inom informationssäkerhetsområdet verkar OECD för samverkan mellan olika typer av aktörer. OECD försöker även verka för utbildning och medvetandegörande hos användare från privatpersoner till offentliga organisationer. Eftersom OECD är en mellanstatlig organisation är det i stort sett det sätt som organisationen kan arbeta på. OECD har inget mandat att tvinga medlemsländerna till ett visst agerande och ländernas delegater har inte heller det i respektive medlemsland. OECD har även sett närmare på och försökt stimulera till mellanstatligt arbete eftersom informationssäkerhet i stor utsträckning handlar om att alla länder deltar.

I arbetet vänder sig OECD huvudsakligen till stater och har endast liten kontakt med företrädare för näringslivet. I den utsträckning man ändå kommunicerar med näringslivet handlar det om stora företag. Små företag anses problematiska på grund av problem med vem som skall finansiera informationssäkerhetsarbetet. Arbetet har låg status och kommer långt ned på listan vid fördelning av medel.

OECD antog den 25 juli 2002, som svar på en uppmaning från USA under 2001, 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 och vänder sig till både stater, offentliga och privata organisationer. Riktlinjerna är formulerade i policytermer och är avsedda att vara övergripande snarare än specifikt inriktande av medlemsländernas strategier.

En plan för genomförande har också tagits fram. Det är upp till regeringen i respektive medlemsland att fatta beslut om hur riktlinjerna skall genomföras. Det är en medveten strategi att inte i detalj föreskriva regler på teknisk eller produktnivå. Medlemsländerna har fått fylla i ett frågeformulär och sammanställningen av svaren har presenterats och diskuterats under en konferens i Oslo i oktober 2003. Den uppfattning som redovisades i Oslo var att många medlemsländer utarbetat en nationell policy, höjt medvetandet, genomfört utbildning och övningar samt inrättat Computer Emergency Response Teams (CERT). Däremot har inte arbetet fortskridit när det gäller s.k. bästa förfaranden (best practices), samarbete mellan olika aktörer och införandet av standarder.

4.2.3 Övriga internationella forum

North Atlantic Treaty Organisation (Nato)

Skydd av kritisk infrastruktur räknas inom Nato till området Informationsoperationer och är sedan 1997 en uppgift för en arbetsgrupp inom Militärstaben. Sedan 1998 har Nato en Information Operation Policy vilket därmed sedan 1999 är ett instrument i Natos planering och övningar.

Nato CIS Operating and Support Agency (NACOSA) har hand om det operativa stödet till alliansen vad gäller underhåll av hård- och mjukvara, personalutbildning, installation av systemkomponenter samt övriga säkerhetstjänster. Som informationsorgan för dessa och andra IT-organ inom området IT-hot mot kritisk infrastruktur, fungerar Nato Consultation, Command and Control Agency (NC3A).

Överenskommelsen Agreement between Parties to the North Atlantic Treaty for the Security of Information är grundlagsdokumentet för att säkerställa skyddet av klassificerad information inom, eller som sänds till Nato. Överenskommelsen ger gemensamma standarder för säkerhetsprövning för utbyte av information mellan medlemsländerna. Det åligger Nato Office of Security att övervaka och pröva dessa säkerhetsstandarder, för att säkerställa en miniminivå av säkerhet.

Inom ramen för samarbetet Partnerskap för fred (PfP) bedrivs arbete med informationssäkerhet bl.a. inom Civil Emergency Planning (CEP) och The Senior Civil Emergency Planning Committee (SCEPC) samt dess underliggande arbetsgrupper – exempelvis Civil Communication Planning Committee (CCPC), Civil Protection Committee(CPC), Industrial Planning Committee (IPC), Food and Agriculture Planning Committee (FAPC), Civil Aviation Planning Committee (CAPC), Planning Board for Inland Surface Transportation (PBIST) och Planning Board for Ocean Shipping (PBOS). De underliggande arbetsgrupperna har getts i uppdrag att studera de generella aspekterna av kritisk infrastruktur, liksom samhälleliga konsekvenser när kritisk infrastruktur inte är tillgänglig, inklusive transportfunktionerna. Det övergripande samordningsansvaret för arbetet med kritisk infrastruktur ligger på SCEPC, men representanter från arbetsgrupperna träffas regelbundet för att diskutera frågor relaterade till kritisk infrastruktur. Detta ger grupperna möjlighet att presentera pågående arbete och planerade aktiviteter, vilket främjar ett närmare samarbete och samordning.

I arbetsgruppen för civila kommunikationer, där informationssäkerhetsfrågorna ingår, deltar Post- och telestyrelsen. Inom området för skydd av kritisk infrastruktur (CIP) har det skapats en ad-hoc grupp under arbetsgruppen Civil Protection, där skydd av kritisk

informationsinfrastruktur (CIIP) ingår som en komponent. I denna arbetsgrupp deltar Krisberedskapsmyndigheten för Sveriges del.

Förenta nationerna (FN)

Förenta nationerna anordnade i december 2003 ett toppmöte om informationssamhället – World Summit on the Information Society. Vid detta möte togs informationssäkerhetsfrågorna specifikt upp i de båda dokument som blev resultatet av toppmötet - en principdeklaration och en handlingsplan.

Vikten av att stärka informationssäkerheten och dessa frågors globala natur lyftes fram. Likaså betonades behovet av internationellt samarbete, samtidigt som åtgärderna måste skydda både data och den personliga integriteten. Dokumenten stödde även Förenta nationernas arbete för att förhindra att IT används för syften som hotar internationell stabilitet och säkerhet.

I handlingsplanen uppmanas staterna att samarbeta med varandra och med den privata sektorn för ökad informationssäkerhet. Bland de åtgärder som lyfts fram märks ökad medvetenhet, utbildning, lagstiftning och informationsutbyte.

Group of Eight (G8)

Sedan 1995 har G8, dvs. Frankrike, Italien, Japan, Kanada, Ryssland, Storbritannien, Tyskland och USA, blivit allt mer involverade i frågor rörande IT-relaterad brottslighet, informationssamhället och skydd av kritisk infrastruktur. 1995 tillsattes en expertgrupp för att utvärdera och se över existerande internationella överenskommelser och mekanismer för bekämpning av organiserad brottslighet, vilket så småningom resulterade i en katalog om 40 rekommendationer. Dessa godkändes vid G8-mötet 1996 i Lyon. Denna s.k. Lyon-gruppen, utgjorde det första internationella politiska forumet som fullt ut erkände betydelsen av högteknologisk kriminalitet. En av de viktigaste uppgifterna för gruppen har blivit att skapa riktlinjer för s.k. bästa förfaranden (best practicise).

G8-länderna har också enats om att en dialog mellan regeringar och den privata sektorn krävs för att bekämpa IT-relaterad brottslighet. Rikskriminalpolisen är Sveriges kontaktpunkt i detta arbete.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN (Internet Corporation for Assigned Names and Numbers) är en privaträttsligt ideell organisation med säte i Kalifornien. Organisationen arbetar för att främja Internets användning och operationella stabilitet.

Organisationen ansvarar för samordning av flera frågor som gäller adresser för Internet Protocol (IP). ICANN har också ansvar för centrala delar av domännamnssystemet (DNS). Systemet används för att underlätta kommunikation med IP och används bl.a. för e-post och andra Internettillämpningar. För att DNS skall fungera måste informationen om de s.k. toppdomänerna (generiska som com-domänen, eller nationella som se-domänen) vara korrekta i den översta nivån i adressystemet (den s.k. rotzonen som finns i rotservrarna). ICANN administrerar ändringar av informationen om toppdomänerna i rotzonen. Det formella ansvaret ligger dock fortfarande på det amerikanska handelsdepartementet (Department of Commerce).

ICANN:s ansvar inom säkerhetsområdet är begränsat. Ansvaret för flera viktiga säkerhetsfrågor ligger hos nätägare, Internetleverantörer, användare av system kopplade till Internet etc. Vad gäller administrationen av DNS och toppdomänerna, för t.ex. Sverige spelar dock ICANN en viktig roll.

I ICANN finns en mellanstatlig rådgivande kommitté, Governmental Advisory Committee (GAC). GAC ger råd till ICANN i de frågor som berör stater, internationella organisationer eller mellanstatliga överenskommelser. Sverige deltar i GAC-arbetet och innehar för närvarande en av viceordförandeposterna. I Sverige svarar Näringsdepartementet för frågor relaterade till ICANN – se vidare ka-pitel 2.

Europarådets cyberbrottskonvention

Redan i slutet av 1980-talet uppmärksammades inom Europarådet att IT-brottslighet var ett område som skulle gagnas av internationellt samarbete. Detta ledde fram till antagande av ett antal rekommendationer och inrättande av en särskild kommitté, ”the Committee of Experts on Crime in Cyberspace”, som fick till uppgift att arbeta fram en konvention om IT-relaterad brottslighet. Kommittén påbörjade sitt arbete i april 1997 och konventionen antogs i november 2001. Konventionen omfattar brottsbeskrivningar, straffprocessuella regler och skapar även ett system för internationellt samarbete. Konventionen innehåller ett antal definitioner, bl.a. av ”datorsystem” och ”datorbehandlingsbara uppgifter”. Definitionerna har legat till grund för, och överensstämmer i princip med, definitionerna i EU:s rambeslut om angrepp mot informationssystem. Samtliga Europarådets medlemsstater deltog i förhandlingarna av texten, tillsammans med Kanada, USA, Japan och Sydafrika. Tillsammans täcker de deltagande staterna en stor del av världens datatrafik. Till konventionen har framförhandlats ett tilläggsprotokoll om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem.

Ett stort antal länder har undertecknat konventionen och ratificering pågår. Inom Justitiedepartementet sker för närvarande en översyn av vilken anpassning som kan behövas i svensk lagstiftning med anledning av konventionen.

5 Kompetensförsörjning

5.1 Säkerhetsmedvetande

Program, produkter och system inom IT-området var före 2000-säkringen, dvs. datoromställningen inför övergången till år 2000, sällan specificerade utifrån ett säkerhetsperspektiv. Säkerhetslösningar applicerades i efterhand, ibland till höga kostnader och med begränsad träffsäkerhet. Arbetet med säkring av data- och kommunikationssystem inför övergången till år 2000 innebar ett trendbrott, inte minst genom att ansvaret för säkringen i såväl myndigheter som näringsliv gjordes till ledningsfrågor för verkställande ledning och styrelse.

Under åren efter 2000-säkringen har säkerhetsmedvetandet höjts. Uppmärksammade erfarenheter av sårbarhet och risker i data- och kommunikationssystem, alltifrån mera triviala störningar till allvarliga intrång, har bidragit till att öka medvetenheten såväl i näringsliv och myndigheter som hos enskilda IT-användare.

Informationssäkerhet handlar inte enbart om att hantera hot. Det ger också möjligheter för såväl den privata som den offentliga sektorn. Utvecklad informationssäkerhet skapar förtroende och möjliggör ett bättre utnyttjande av informationsteknikens potential. Det bidrar till en god etik genom att förhindra otillbörlig åtkomst av information och pengar.

Det finns skäl att bedöma behovet av särskilda insatser för en bred påverkan av attityder till informations- och IT-säkerhet, såväl beträffande informationssystem i arbetslivet som i hushållens ökade användning av dator- och IT-system. Främst gäller det att öka medvetenheten om sårbarhet och risker, men också om metoder

och åtgärder för att skapa säkrare system. Det finns t.ex. skäl att värdera behovet av enklare testhjälpmedel för att underlätta en förbättrad säkerhet.

Utan säkerhetsmedvetande är flertalet åtgärder för att skapa en rimlig säkerhetsnivå av begränsat värde. Det finns därför anledning att överväga åtgärder för att bygga in säkerhetsmedvetande som ett centralt inslag redan i skolans grundläggande data- och IT-utbildning. Det kan gälla såväl på grundskole- som på gymnasienivå.

5.2 Behov av kvalificerad utbildning och forskning

För högskolenivån avser utredningen att i det fortsatta arbetet belysa tillgången till säkerhetsinriktade ämnen inom bl.a. tekniska och ekonomiska utbildningar. Det finns skäl att som del i samhällets säkerhetsförebyggande arbete överväga att bygga in rekommendationer om inslag av utbildning om sårbarhet och säkerhet som en normal del i grundutbildningarna för t.ex. civilingenjörer, civilekonomer och i vissa andra akademiska examina.

Syftet är i så fall i första hand att fördjupa säkerhetsmedvetandet men också att ge en grund för att lära känna administrativa och tekniska metodfrågor för risk- och sårbarhetsanalys, utveckla beställarkompetens vid upphandling och inköp och utveckla ett kunnande inom säkerhetsområdet som är användbart i arbetslivet.

Som exempel på existerande utbildning kan nämnas att den gemensamma institutionen för data- och systemvetenskap vid Stockholms universitet och Kungl. Tekniska högskolan utbildar civilingenjörer och systemvetare i informationssäkerhet och IT-säkerhet och riskhantering. Årligen går ett antal studenter ut med säkerhet som huvudämne i magister- och civilingenjörsexamen. Utbildningen omfattar såväl matematiska (kryptering) som tekniska och praktiska (säkerhetsprogramvaror, administrativ och organisatorisk säkerhet) områden.

För närvarande bedrivs vid institutionen utöver den ordinarie säkerhetsutbildningen ett magisterprogram för ett sextiotal internationella studenter. Ett tjugotal doktorander finns i säkerhetsrelate-

rade ämnen. Av forskarna och lärarna på institutionen har huvuddelen disputerat i säkerhet.

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 ett större sammanhang, informationssäkerhet. I flera utbildningar, t.ex. 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 de? Vilka policy och rutiner bör skapas? IT-säkerhet är en del av skyddet, men endast en del.

En särskild svårighet finns i mötet mellan juridiken och tekniken. I den privata sektorn blir detta tydligt vid upprättande 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.

Utöver den interna utbildning som bedrivs, kan nämnas att ett nytt program med inriktning på IT-säkerhet och delvis på IT-forensisk (kriminalteknisk) verksamhet har startats vid Blekinge Tekniska Högskola (BTH). Programmet är en akademisk 40-poängsutbildning på halvfart, riktad mot redan yrkesverksamma. Personal från Rikskriminalpolisen, Säkerhetspolisen och Polishögskolan har deltagit vid planeringen av utbildningen. För närvarande deltar bl.a. ett antal poliser i den första kursomgången.

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. Professorerna i rättsinformatik är på olika sätt engagerade i säkerhetsfrågor.

Exempel på aktuella teman i IRI:s verksamhet är personuppgiftsskyddets förändrade förutsättningar vid nätbaserade tjänster, rättslig riskanalys, säker dokumentadministration , access till myndighetsinformation, samt rättsligt skydd av informationsinfrastrukturen. De båda sistnämnda är doktorandprojekt stödda av Verket för innovationssystem (Vinnova). Senare under 2004 arrangerar IRI en nordisk rättsinformatikkonferens som helt kommer att ägnas åt rättsliga aspekter på informationssäkerhet.

Även inom medicinska och sociala utbildningar finns behov av kompetens i informationssäkerhet, bl.a. ur integritetsperspektiv.

I detta sammanhang bör också framhållas att den största delen 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 utbildning. Utbudet av dessa utbildningar är omfattande. De uppdateras kontinuerligt och är i praktiken en del av IT-utvecklingen.

Forskning behövs för att utveckla informationssäkerheten, både grundforskning och forskning om tillämpade metoder, ledningssystem och andra system, program och produkter. Den behövs också för att utveckla kompetens och stimulera kvalitet i utbildningen. Det gäller både för den offentliga verksamheten och för näringslivet.

Alla med sektorsansvar inom området informationssäkerhet måste känna ansvar för forskningen inom den egna sektorn.

Krisberedskapsmyndigheten har ett särskilt ansvar inom forskningsområdet att stimulera, initiera, beställa och delvis finansiera forskning inom informationssäkerhet. Det gäller både forskning inom det allmänna universitets- och högskoleområdet och inom ramen för Försvarshögskolans och Totalförsvarets forskningsinstituts verksamhet. Detta ansvar kan behöva förtydligas ytterligare.

Försvarssektorn har traditionellt satsat betydande resurser på forskning och studier. Det militära försvaret har härvidlag varit starkt prioriterat resursmässigt, i enlighet med den hotbild som förevarit under efterkrigstiden. Dagens säkerhetspolitiska utma-

ningar kan dock inte lösas enbart med militära medel. Säkrandet av rikets ledning vid en svår nationell påfrestning 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.

Utredningen avser att skaffa sig en uppfattning om omfattning och inriktning på dagens forskning i informationssäkerhet och värdera behovet av ytterligare stimulans.

5.2.1 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 bl.a. forskning och studier genom sitt Centrum för Informationsoperationsstudier (CIOS). Vid Försvarshögskolan utvecklas även Informationsoperationer som ett akademiskt ämne i internationell samverkan med bl.a. University of St. Andrews i Skottland och National Defence University i USA. Aktuella delområden är informationsterrorism, policy och skydd av nationell infrastruktur på informationsområdet, varseblivningsanalys och psykologiska operationer samt metodik för omvärldsanalys.

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 nät-

verksattacker. 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 och underrättelseorienterade frågeställningar. Försvarshögskolan har dock inget operativt ansvar inom området informationsoperationer.

5.2.2 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 bl.a. Försvarsdepartementet, Utrikesdepartementet, Försvarsmakten, Krisberedskapsmyndigheten och Försvarets materielverk.

Vid avdelningen för försvarsanalys genomförs studier och forskning inom området informationssäkerhet på olika systemnivåer. Uppdragen har bl.a. varit orienterade mot säkerhetspolitiska bedömningar, hotbildsanalyser, framtidsstudier och samhällsorienterade sårbarhetsanalyser. Verksamheten har även omfattat system-

nära säkerhetsanalyser och scenarion av IT-system inom t.ex. vattenförsörjning, telekommunikation, elproduktion och drivmedelsförsörjning. Under senare år har kunskapsutveckling skett inom området säkring av viktig infrastruktur, där 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.

5.3 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 t.ex. 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 kompe-

tens 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. Idag ser bilden annorlunda ut, men inte beroende av 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 idag 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 idag via Internet. IT ger också möjligheter att kryptera kommunikation och hårddiskar utan att egentligen ha någon teknisk kompetens på området.

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. 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.

Behovet av kryptokompetens i samhället är alltså stort och växande. Kompetenskraven har höjts kraftigt under senare år. Den fortsatta utredningen avser att redovisa förslag till åtgärder för hur detta behov skall kunna tillgodoses.

5.4 Kompetens hos beställare och leverantörer

5.4.1 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. När beställaren är medveten om vad som krävs av ett bra informationssäkerhetsskydd, är det också möjligt att definiera skyddet, anpassa det och upphandla.

Här bör övervägas vilket ansvar samhället har för att utveckla beställarkompetens och eventuella former för en sådan kompetensutveckling. Sannolikt kommer en höjd 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 ytterligare starka drivkrafter finns för att utveckla kompetensen. Näringslivets behov av grundläggande kompetensförsörjning bör därför också ha betydelse för utformningen av en nationell strategi.

Beställarkompetensen 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 bör gälla för affärsdrivande verk, kommuner och landsting och inom näringslivet.

Företeelsen outsourcing, dvs. att lägga verksamhet på entreprenad, ökar behovet av beställarkompetens. Under senare år har det blivit allt vanligare att lägga hela eller delar av informationstekniken på entreprenad till andra företag med specialkompetens. Utredningen avser att belysa denna företeelse, som i många fall kan vara ett instrument för att till rimliga kostnader tillföra kompetens om informationssäkerhet och IT-system, samtidigt som det också kan medverka till att på längre sikt avhända myndigheter, kommuner

eller företag grundläggande kompetens beträffande funktion och innehåll i IT-system och därigenom också informationssäkerhet.

Beställarrollen behöver dock förtydligas även vid egen drift.

Det gäller också att redan i beställarskedet säkerställa att inte luckor uppstår i informationssäkerheten, vare sig i den administrativa eller i den tekniska hanteringen.

Utveckling av IT-säkerhet med stöd av internationellt accepterad standard är en metod för att skapa tillit och förtroende såväl inom en organisation som mellan olika parter.

ISO/IEC IS 15408 Evalueringskriterier för IT-säkerhet, ofta kallad Common Criteria, behandlar kravspecifikation, granskning och evaluering av teknisk IT-säkerhet. Den är också ett viktigt exempel på internationell samverkan. Syftet med den överenskomna standarden är bl.a. att tillse att evalueringar utförs i väldefinierade, internationellt accepterade former.

En metod att ytterligare utveckla beställarkompetens kan vara att använda en gemensam standard 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.

En sådan standard är SS 627799, Ledningssystem för informationssäkerhet, som har viss tillämpning internationellt. Den blev en ISO-standard i december 2000 (ISO 17799). Bland länderna i ISO-samarbetet använder Storbritannien, Australien och Nya Zeeland standarden fullt ut. Kanada, Japan och Nederländerna har också kommit en bit på väg. Tyskland och Frankrike använder egna anpassningar av standarden.

Krisberedskapsmyndigheten definierar i sina rekommendationer en basnivå för IT-säkerhet, BITS, som minst måste uppnås för IT-system, dvs. som bedöms nödvändiga för att upprätthålla en organisations normala verksamhet även under fredstida kriser. Om denna basnivå är tillräcklig skall avgöras genom en risk- och sårbarhetsanalys i varje enskilt fall.

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. Enligt Krisberedskapsmyndighetens bedömning krävs en omfattande insats för att uppfylla SS 627799. Ambitionen är att få BITS att konvergera mot informationssäkerhetsstandarden i de delar där parallellitet finns. Grundtanken att definiera en lägsta nivå för IT-säkerheten kvarstår.

Standarden SS 627799 (ISO 17799) har ambitionen att omfatta hela informationssäkerhetsbegreppet, dvs. inte endast IT-säkerhet som BITS gör.

Statskontorets mall, OffLIS, för utformning av en organisations regelverk som ”Ledningssystem för informationssäkerhet” baserar sig på standarden ISO 17799 och är utformad för att ge vägledning i första hand för utvecklingen av e-tjänster inom konceptet för 24-timmarsmyndigherna.

Varje standard måste tas på allvar. Den får aldrig tillåtas bli enbart en etikett som man visar upp utåt för att förmedla en bild av säkerhet och tillit. Utredningens avsikt är att värdera om en mera generell användning av informationsstandard är en bra och resurseffektiv metod för att utveckla beställarkompetens och skapa en höjd, tillika mera gemensam säkerhetsnivå vad gäller informationssäkerhet.

Särskild uppmärksamhet bör ägnas kompetensen i avtalsfrågor. Mötet mellan teknik och juridik, särskilt när det gäller informationssäkerhet är komplicerat. Det kan kräva utvecklingsinsatser. Utredningen avser att fördjupa analysen av behoven i denna del.

5.4.2 Leverantörskompetens

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.

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. Det är därför ett nationellt intresse att tillgodose samhällets behov av leverantörskompetens inom området.

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. Utredningen avser att skaffa sig en uppfattning om utbudet av utbildningar inom informationssäkerhet och kvaliteten på dessa samt värdera behovet av ytterligare utbildningar inom området.

5.5 Certifiering och revision

5.5.1 Certifiering

Certifiering av IT-säkerhet med stöd av internationellt accepterade standarder behandlades av Sårbarhets- och säkerhetsutredningen (SOU 2001:41). Det är som utredningen framhöll ett viktigt område för att skapa tillit och förtroende såväl inom en organisation som mellan olika parter:

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

När säkerheten i en produkt eller i ett system granskas, krävs en beskriven metodik. Vid informell teknisk granskning kan annars

svårigheter uppstå att påvisa vad granskningen omfattat och vilken metodik som tillämpats. Ofta uppstår brister i dokumentationen.

Regeringen har uppdragit åt Försvarets materielverk att etablera en certifieringsfunktion för IT-säkerhet. Uppbyggnaden har av olika anledningar tagit tid. Ännu är exempelvis inga evalueringsföretag licensierade. Några certifikat har därigenom ännu inte heller kunnat utfärdas. Processen med uppbyggnad pågår dock. Utredningen har till uppgift att följa denna process som syftar till att underlätta upphandling av säkra produkter och system för myndigheter och andra beställare.

5.5.2 Kontroll och rådgivning enligt säkerhetsskyddslagen

Säkerhetspolisen och Försvarsmakten ansvarar för att kontrollera säkerhetsskyddet inom sina respektive ansvarsområden. Vid alla kontroller ingår IT-säkerhet 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 IT-säkerhet 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 berörda kontrollerade organisationer om behovet av tillfredsställande skydd, bl.a. för informationssäkerhet.

5.5.3 Revision

Vid 2000-säkringen visades att revision är en konstruktiv metod för säkerhetsutveckling också inom området IT-säkerhet. Från att tidigare inte närmare ha belyst området och inte heller ansett att informationssäkerhet eller IT-revision varit en del av den lagstadgade revisionen håller nu revisionsområdet med såväl internrevision som Föreningen Auktoriserade Revisorer, FAR, på att ändra synsätt.

Under det senaste året har en ny revisionsstandard, RS 401 Revision i en datoriserad informationssystemmiljö, införts som gäller

informationssäkerhet och granskning av datoriserade miljöer. Den gäller från och med den 1 januari 2004 och skall tillämpas vid revisionen av 2003 års räkenskaper för företag. RS 401 överensstämmer med den internationella revisionsstandarden ISA 401.

Syftet med denna revisionsstandard är att lägga fast standarder och ge vägledning när en 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.

I RS 401 konstateras att datoriserade informationssystem kan erbjuda företagsledningen en rad analysverktyg, som kan användas för att granska och övervaka företagets verksamhet. Tillgången på sådan extra kontrollmöjligheter kan, om de utnyttjas, tjäna till att förstärka hela den interna kontrollstrukturen. Både de risker och de kontroller som blir resultatet av dessa egenskaper som kännetecknar datoriserade informationssystem kan påverka revisorns riskbedömning samt granskningsåtgärdernas karaktär.

Den nya revisionsstandarden tillämpas ännu inte vid Riksrevisionens revision av statliga myndigheter. Utredningen anser att det är önskvärt att så snarast blir fallet. Enligt uppgift kommer en översyn av Riksrevisionens regler i relation till RS (Revisionsstandard i Sverige) att påbörjas under våren.

Den nya revisionsstandarden ställer både krav på kompetensutveckling inom revisionsområdet samtidigt som en utveckling av revision inom dessa områden kan komma att medverka till kompetensutveckling, inte minst på ledningsnivå inom företag och myndigheter.

Utredningen avser att belysa möjligheterna till kompetensutveckling genom en mera generell användning av revisionsinstrumentet inom informationssäkerhet och IT-säkerhet.

5.6 Fortbildning och erfarenhetsöverföring

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. Det gör att behovet av fortbildning i frågor som rör informationssäkerhet och IT-säkerhet är mycket omfattande.

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. I många fall handlar det om kvalificerade fortlöpande utbildningsbehov. Det kan gälla bl.a. utbildning i risk- och sårbarhetsanalys liksom utbildning inom själva riskhanteringsprocessen. I andra fall kan det röra sig om bredare fortbildning med tonvikt på säkerhetsmedvetande.

Även då informationsfunktioner och IT-funktioner läggs på entreprenad kan behovet av fortbildning för den egna personalen i frågor rörande informationssäkerhet vara betydande.

Informationssäkerhetsutredningen kommer att följa Försvarets materielverks arbete med att skapa en certifieringsprocess, liksom verksamheten vid den teknikkompetensfunktion som etablerats vid Försvarets radioanstalt och den rikscentral för IT-incidentrapportering, Sitic, som etablerats vid Post- och telestyrelsen samt den funktion för omvärldsanalys som etablerats inom Krisberedskapsmyndigheten. Avsikten är bl.a. att värdera behovet av och möjligheterna till kunskapsöverföring från dessa verksamheter till kompetenshöjande fortbildning inom främst myndigheter och andra med ansvar för samhällskritisk infrastruktur.

6 Utredningens överväganden

I detta kapitel uppmärksammar utredningen ett antal områden som identifierats vara av särskild vikt och betydelse för det fortsatta arbetet, och som måste beaktas vid utformningen av utredningens förslag i slutbetänkandet den 6 maj 2005

6.1 Statens roll och ansvarsfördelning mellan aktörer

Med utgångspunkt i generella motiv för offentliga åtaganden inom olika områden har bl.a. Sårbarhets- och säkerhetsutredningen (SOU 2001:41) behandlat frågan om statens roll och möjliga uppgifter för de offentliga organen inom krishanteringsområdet. Utredningen konstaterar liksom Sårbarhets- och säkerhetsutredningen att motiven för det offentliga åtagandet visserligen i regel har sitt ursprung i ekonomiska teorier om statens roll i samhällsekonomin, men att det i många fall är möjligt att tillämpa de resonemang som förs i sådana sammanhang också på icke-ekonomiska problemställningar. De offentliga aktörerna täcker alltså behov och står för kollektiva nyttigheter som marknaden av olika skäl inte kan tillgodose. Försvar, polisväsende och räddningstjänst brukar anföras som typiska exempel på kollektiva nyttigheter där samhället historiskt haft en uppgift och roll, genomfört investeringar och utfärdat handlingsregler, exempelvis genom lagar som reglerar plikttjänstgöring, våldsanvändning, intrång i annans rätt etc. Utredningen anser att det på motsvarande sätt finns motiv för ett offentligt engagemang när det gäller informationssäkerhet.

Om det offentliga inte engagerar sig inom dessa områden kan man alltså befara att satsningarna annars blir otillräckliga. Medborgarna och många andra aktörer inom olika verksamhetsområden kan sägas ha svårt att överblicka och värdera de risker som finns, och har också svårt att förbereda sig för egen del om offentliga organ inte

gör riskbedömningar och förmedlar resultatet av dessa. Huvuddelen av informationssäkerhetsarbetet måste dock utföras av dem som har ansvar för IT-systemen. Det offentligas roll måste analyseras och avgränsas till de områden där det offentligas roll är avgörande eller nyttan är så stor att ett offentligt ingrepp kan motiveras. Det skulle kunna vara att stimulera till eller ställa krav på att säkerhetsåtgärder vidtas och att utöva en aktiv tillsyn över efterlevnaden av gällande bestämmelser inom området. Grundläggande säkerhetskrav skulle kunna ges lagstöd och preciseras i föreskrifter. I vissa fall kan det bli nödvändigt att offentliga organ tar ansvar för att finansiera och producera säkerhetsåtgärder. Till detta bör läggas att de offentliga organen i sig, och i allt större utsträckning, också är aktörer inom området.

Mot denna bakgrund och grundat även på de internationella erfarenheter utredningen tagit del av, redovisar utredningen i det följande, 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:

- identifiera, utvärdera och presentera en översikt av hotbilden
- utarbeta en sårbarhetsbedömning på nationell nivå
- tydliggöra en nationell policy/strategi
- föreslå och förmedla grundläggande regelverk (föreskrifter, rekommendationer med lämpliga standarder som grund)
- råd och information till allmänheten
- generella råd och stöd till myndigheter
- särskilda råd och stöd till särskilt viktiga myndigheter eller avseende särskilt viktiga system
- skydd av IT-system inom samhällsviktiga system
- förebygga, upptäcka, utreda och lagföra IT-relaterad brottslighet
- skydd mot informationsoperationer
- kryptografi för särskilt viktiga myndigheter och särskilt viktiga system
- standarder (ledningssystem för informationssäkerhet; tekniska krav på funktioner och evaluering; certifieringskrav, m.m.)

- varningar och information om IT-säkerhetsincidenter (CERT)
- kvalificerat teknikstöd
- föreskriftsrätt
- säkerhetsskydd
- signalskyddstjänst

Det finns vidare flera tänkbara målgrupper för informationssäkerhetsarbetet, som stora användare av IT-system och ansvariga för särskilt viktiga system, m.fl. En övergripande indelning kan dock vara:

- statlig förvaltning
- kommuner och landsting
- näringsliv
- allmänhet

Ansvariga statliga myndigheter kan också ha olika roller:

- tillsyn
- främjande
- producent
- konsument

Det finns också flera olika sätt att utöva det övergripande statliga ansvaret:

- regelstyrning
- tillsyn
- budgetstyrning
- myndighetsstyrning

Med utgångspunkt i dessa arbetsuppgifter, målgrupper, roller och styrinstrument har utredningen konstaterat att informationssäkerhetsarbetet i andra länder har organiserats på några principiellt skilda sätt.

Utredningen har vidare följt utvecklingen av informationssäkerhetsfrågorna i Sverige. Regeringen anmälde i propositionen Samhället säkerhet och beredskap (prop. 2001/02:158) att fyra myndigheter avsågs ges särskilda uppgifter inom informationssäkerhetsområdet. Dessa var Krisberedskapsmyndigheten, som skulle få

ett sammanhållande myndighetsansvar för samhällets informationssäkerhet, Förvarets materielverk, som skulle inrätta en certifierings- och evalueringsfunktion enligt Common Criteria, Post- och telestyrelsen, som skulle hantera uppgifter om IT-incidenter (en rikscentral för IT-incidentrapportering) samt Förvarets radioanstalt, som skulle tillhandahålla teknikkompetens inom området.

Regeringen har vid flera tillfällen påpekat att ansvarsprincipen gäller och att de utpekade myndigheterna inte på något sätt övertagit ansvaret från övriga myndigheter.

Post- och telestyrelsen startade sitt arbete vid halvårsskiftet 2002, Krisberedskapsmyndighetens Informationssäkerhetsenhet påbörjade sitt arbete vid halvårsskiftet 2003, medan övriga myndigheter började bygga upp verksamheten vid årsskiftet 2002/03. Myndigheternas arbete har inledningsvis fokuserat på att närmare definiera innebörden av uppgifterna, rekrytera personal och att bygga upp kontaktnät nationellt och internationellt.

Krisberedskapsmyndigheten inrättade inom ramen för sitt ansvarsområde en samverkansgrupp mellan de myndigheter som tilldelats särskilda roller, dvs. Krisberedskapsmyndigheten, Försvarets radioanstalt, Post- och telestyrelsen och Försvarets materielverk. Polisen anslöts till gruppen då polisen genom sitt ordinarie myndighetsansvar på det brottsförebyggande och brottsbekämpande området, samt sitt särskilda ansvar när det gäller säkerhetsskydd, kunde tillföra viktiga aspekter. Vidare ansågs Statskontoret ha en viktig roll inom informationssäkerhetsområdet, bl.a. när det gäller 24-timmarsmyndigheten, och Försvarsmakten utgöra en betydelsefull aktör, varför även dessa anslöts till gruppen som idag går under benämningen Samverkansgruppen för informationssäkerhet (SAMFI).

Utredningen har följt Krisberedskapsmyndigheten, Försvarets radioanstalt, Post- och telestyrelsen och Försvarets materielverk i uppbyggnaden av de olika verksamheterna. Utredningen har funnit att det är för tidigt att i nuläget närmare värdera det arbete som hittills genomförts. Utredningen kan dock konstatera att den inriktning som beslutades under 2002 om att ge de fyra myndigheterna ett särskilt ansvar inneburit att verksamheten på ett påtagligt sätt kommit igång och att förutsättningarna för en god informationssäkerhet förbättrats.

Utredningen konstaterar dock att det under det gångna året förekommit diskussioner rörande gränsdragningsfrågor, dels om relationen mellan de fyra särskilt utpekade myndigheterna, dels om dessa myndigheters relation till andra myndigheter som är verksamma inom informationssäkerhetsområdet, t.ex. Statskontoret, Styrelsen för ackreditering och teknisk kontroll (SWEDAC), Säkerhetspolisen och Försvarsmakten. Oklarheterna om gränsdragning gäller i vissa fall instruktioner för myndigheterna, men framför allt den praktiska uppdelningen av arbetet. Vidare är den operativa ansvarfördelningen och samordningen vid krishantering oklar.

I utredningsarbetet har också framkommit 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 har också noterat att informationssäkerhetsarbetet av många uppfattas som alltför präglat av historiskt viktiga kopplingar till totalförsvarsverksamheten. Utredningen anser i det sammanhanget det som mycket väsentligt att synen i stort på informationssäkerheten i samhället förändras, och att det blir tydligt att informationssäkerhetsarbetet gäller hela samhället och inte bara försvarsrelaterade myndigheter.

Utredningen kommer i det fortsatta arbetet med överväganden om fördelning av ansvar inom informationssäkerhetsområdet att ha som utgångspunkt 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 är väsentligt att arbetet verkar förebyggande, men det måste också finnas instrument när samhället utsätts för olika informationsattacker.

6.2 Analys av kritisk infrastruktur

Infrastruktur är en kombination av administrativa och organisatoriska åtgärder och de tekniska anläggningar och utrustningar som behövs för att ett samhälle skall kunna fungera på ett tillfredsställande sätt. Ett samhälle behöver olika typer av infrastruktur, som samverkar med varandra, för att fungera. Utredningen anser att myndigheternas roller och ansvar för informationssäkerheten bör

förändras utgående från analyser av vad som är kritisk/samhällsviktig infrastruktur.

Utgångspunkten för informationssäkerhetsarbetet har fram till början av 2000-talet varit situationsberoende, i meningen att ansvar, åtgärder, finansiering, m.m. 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. Detta förhållande kvarstår i viss utsträckning, vilket framgår av de myndighetsinstruktioner som redovisas i kapitel 3. Således har t.ex. Statskontoret och Krisberedskapsmyndigheten likartade eller jämförbara uppgifter rörande informationssäkerhet, men för olika situationer.

Utredningen konstaterar att en sådan situationsberoende uppdelning inte är ändamålsenlig eftersom den leder till oklara ansvarsförhållanden, att resurser som tillskapas inte utnyttjas fullt ut eller att nödvändiga åtgärder inte kan genomföras. Ett exempel på vad denna situationsberoende uppdelning innebär i form av begränsningar respektive behov av dubblering av resurser är möjligheterna att pröva eller öka informationssäkerheten i elsystemet. Med dagens regelsystem kan s.k. aktiv IT-kontroll genomföras vid myndigheter och statligt ägda bolag. Det innebär att det statligt ägda bolaget Vattenfall kan pröva informationssäkerheten i sina system med stöd av de resurser som finns vid Försvarets radioanstalt, samtidigt som privata aktörer på elmarknaden, som i lika hög grad utgör en viktig del av den kritiska infrastrukturen, formellt inte ges denna möjlighet.

Utgångspunkten bör enligt utredningens uppfattning i stället vara en funktionsorienterad uppdelning. Ur ett statligt perspektiv är det således upprätthållande av kritisk infrastruktur som bör vara utgångspunkten för vilket ansvar staten har för informationssäkerheten.

6.3 Begrepp och definitioner

I arbetet med att skapa en enhetlig begreppsapparat, som både är funktionell och samtidigt förankrad bland aktörerna inom informationssäkerhetsområdet, har utredningen funnit att det är väsentligt att beakta både de legala och tekniska perspektiven. En av utred-

ningens utgångspunkter har därför varit att söka lämpliga legaldefinitioner som skulle kunna koppla samman de övergripande begreppen och definitionerna med de tekniska och administrativa som redan finns etablerade. Ett viktigt skäl till detta är 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.

Som tidigare anförts har föregångaren till det legala begreppet informationssäkerhet, dvs. sekretesskydd, till stora delar handlat om regler för fysisk hantering av hemliga handlingar i pappersform. Med handling avses enligt tryckfrihetsförordningen, förutom framställning i skrift eller bild, även upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniska hjälpmedel. I förarbetena till säkerhetsskyddslagen anförde regeringen att utvecklingen på informationsteknikens område har medfört att skyddet av sekretessbelagd information har fått en annan dimension än tidigare. Detta markerades i säkerhetsskyddslagen genom att ordet sekretesskydd byttes ut mot informationssäkerhet (prop. 1995/96:129, sid. 27). På så vis kan det sägas att lagstiftaren i syfte att skydda grundläggande värden har skapat begrepp och definitioner ovanifrån.

Framväxten av moderna IT-system har genererat begrepp och definitioner i takt med behoven och de tekniska möjligheterna. Dessa begrepp har huvudsakligen utvecklats av FoU-ansvariga, producenter, leverantörer, systemkunniga, tekniker, m.fl. Begreppen kan på så vis sägas ha formulerats underifrån.

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. Begrepp och definitioner som rör informationssäkerhet måste konkretiseras ytterligare för att kunna tjänstgöra som verktyg. Regelverket bör i högre grad anpassas till hantering av handlingar i IT-system. Utredningen har erfarit att detta är ett av syftena med den pågående översynen av Rikspolisstyrelsens föreskrifter om säkerhetsskydd (RPS FS 1996:9). Vid översynen kommer hänsyn även att tas till EU:s säkerhetsbestämmelser.

Enligt utredningen förefaller det som att EU (och OECD) har modernare bestämmelser och tydligare visioner för informations-

säkerhetsarbetet 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.

EU:s säkerhetsbestämmelser omfattar i princip all verksamhet inom EU och dess medlemsstater. I säkerhetsbestämmelserna finns ett särskilt avsnitt som behandlar informationssäkerhet.

Enligt utredningens mening borde EU:s arbete inom informationssäkerheten kunna utgöra en utgångspunkt för en gemensam syn på begrepp och definitioner som grund för nationella bestämmelser om informationssäkerhet.

De begrepp och definitioner som redovisats i SIS Handbok 550: Terminologi för Informationssäkerhet är väl förankrade så väl internationellt som nationellt. SIS-projektet kan därmed sägas representera ett underifrånperspektiv på definitioner. Möjligen kan enskilda val av begrepp diskuteras, men inte helheten. Indelning i administrativ respektive teknisk informationssäkerhet kan säkert ligga till grund för fortsatt arbete.

BITS är ett intressant exempel på hur informationssäkerhetsarbetet kan konkretiseras med stöd av precisa författningar, i detta fall 11 § förordningen om åtgärder för fredstida krishantering och höjd beredskap (2002:472). En avgörande begränsning är att föreskrifterna avser förhållanden inför och under höjd beredskap, vilket minskar kretsen av berörda myndigheter.

Formuleringen i rådets säkerhetsbestämmelser, att säkerheten syftar till att främja tillväxt, konkurrens och välfärd, är i det sammanhanget intressant. I direktivet har den nya tekniken fångats in med följande formulering ”uppgifter som lagras, bearbetas eller överförs i elektronisk form”. I detta sammanhang skall informationssäkerheten uppfyllas genom krav på konfidentialitet, okränkbarhet och tillgänglighet. Kravet på okränkbarhet och tillgänglighet gäller all

informationshantering, oavsett om uppgifterna är hemliga eller inte.

Med denna grundläggande definition av informationssäkerhet inom EU som utgångspunkt skulle bestämmelser kunna konkretiseras utifrån den administrativa och tekniska hierarki som utarbetats inom SIS-projektet. Regeringen har vidare möjligheter att genom förordning 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.

6.4 Författningar

6.4.1 Möjligheter att bedriva ett effektivt informationssäkerhetsarbete

Med utgångspunkt i dagens lagstiftning har de tillfrågade myndigheterna analyserat sina möjligheter att bedriva ett effektivt informationssäkerhetsarbete. För närvarande upplever flera myndigheter att begreppet ”rikets säkerhet” i kap. 2 § 2 sekretesslagen har en för snäv tolkning. Mycket av för samhället viktig verksamhet faller utanför säkerhetsskyddslagen eftersom den inte rör rikets säkerhet enligt dagens tolkning av begreppet.

Begreppet bör enligt dessa tolkas eller omformuleras 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.

Det finns inte någon legaldefinition av begreppet rikets säkerhet utan det måste tolkas utifrån förarbeten och praxis. Allmänt kan begreppet sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket. Skyddet för den yttre säkerheten tar i första hand sikte på totalförsvaret. 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. 22f).

Begreppet rikets säkerhet används på olika håll i lagstiftningen bl.a. i brottsbalken, sekretesslagen (1980:100) och säkerhetsskyddslagen (1996:627). En ändring av begreppets innebörd skulle således kunna få långtgående konsekvenser och bl.a. påverka det straffbara området för t.ex. spioneribrott.

Vid tolkningen av begreppet rikets säkerhet måste hänsyn också tas till den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Vissa av de rättigheter som konventionen tillförsäkrar får inskränkas under vissa förhållanden, t.ex. om det har stöd i lag och det ”i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet…”. Sålunda får t.ex. rätten till skydd för privat- och familjeliv inskränkas, liksom yttrandefriheten. Sverige bör inte gå längre i sin tolkning av när inskränkningar är tillåtna än vad som accepteras av den Europeiska domstolen för de mänskliga rättigheterna.

Ett flertal myndigheter pekar på problem med hanteringen av uppgifter som omfattas av sekretess men som inte rör rikets säkerhet och som därmed faller utanför säkerhetsskyddslagens tillämpningsområde. Ett exempel är skydd av kritisk infrastruktur. Även bristen på sekretess för IT-säkerhetsanalyser och IT-incidentsrapporter innebär ett problem, då osäkerheten på området hindrar att rapporter upprättas eller lämnas vidare.

Det kan alltså finnas anledning att analysera säkerhetsskyddslagen närmare i det fortsatta arbetet. För det fall att utredningen kommer fram till 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.

Ett sätt att kartlägga i vilken omfattning angrepp riktade mot IT-system förekommer är att sätta upp detekterande system. Dessa innehåller ingen information som kan tänkas eftersökas av någon på legal väg, och därmed kan genom intrången angriparnas tillväga-

gångssätt och mål, samt verktyg som används studeras. De rättsliga förutsättningarna för användandet av denna metod och andra närbesläktade metoder bör undersökas. En liknande fråga är den som rör förutsättningarna att bedriva aktiv IT-kontroll av egna IT-system i syfte att påvisa brister i säkerheten i nätverk, brandväggar etc. Här aktualiseras såväl lagen (2003:389) om elektronisk kommunikation (EkomL) som personuppgiftslag (1998:204) och relevanta bestämmelser i brottsbalken.

För att möta de kvalificerade IT-relaterade hoten (även traditionell underrättelseinhämtning) krävs ett systematiskt informationssäkerhetsarbete på en övergripande nivå och i de organisationer som är utsatta för hot. Det spänner över hela området med tekniska och administrativa åtgärder. Ett sätt upptäcka externa hot är att komplettera organisationers grundskydd med system som på ett strukturerat sätt samlar in och analyserar trafikdata som rör kritisk infrastruktur. Som jämförelse kan nämnas Norges Varslingssystem for Digital Infrastruktur, (det så kallade VDI-projektet), som samlar den typen av data för kritiska infrastrukturer). Ett sådant system förlorar delvis sin betydelse om det inte ingår i en helhet med det övriga informationssäkerhetsarbetet.

När det gäller brottsförebyggande verksamhet och lagföring av brott skapar den snabba tekniska utvecklingen på området särskilda svårigheter eftersom lagstiftningen bör vara så teknikneutral som möjligt samtidigt som den måste uppfylla de krav på tydlighet som ställs på strafflagstiftning. 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 med relevans för dessa frågor.

Utredning av IT-relaterad brottslighet ger kunskaper om bl.a. tillvägagångssätt och aktörer, vilket är av stort värde vid utformningen av olika skyddsåtgärder. En effektiv lagföring av IT-relaterad brottslighet är viktig för att minska benägenheten att begå sådana brott. Möjligheten att spåra angrepp är en viktig komponent, och kräver att trafikuppgifter finns bevarade och tillgängliga. För närvarande är det tillåtet för teleoperatörer att lagra trafikuppgifter för vissa ändamål, men det finns ingen skyldighet att göra så.

Ett av syftena med lagen om elektronisk kommunikation (EkomL) är att denna skall omfatta alla nätverk för överföring och tillhörande tjänster och således vara teknikneutral. Ett flertal bestämmelser synes dock vara svårapplicerade på annan teknik än traditionell telekommunikation. Post- och telestyrelsen har med den nya lagen fått nya instrument för att uppnå målet om säkra kommunikationer. I EkomL har kraven på dem som tillhandhåller taltelefonitjänst skärpts jämfört med telelagen. Samtidigt har möjligheterna att ställa krav på förebyggande åtgärder för andra kategorier av operatörer försämrats jämfört med telelagen. Inom Post- och telestyrelsen analyseras vilka möjligheter lagen ger att uppnå önskvärda mål om säkra kommunikationer, bl.a. undersöks vilka möjligheter som finns att ställa krav på förebyggande åtgärder för Internetoperatörer. Post- och telestyrelsens bedömning är att EkomL i vissa stycken ger sämre verktyg än telelagen för att säkerställa driftsäkra kommunikationer inom hela området för elektronisk kommunikation. Förslag om lagändringar kan bli aktuella. När det gäller de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i uppgifter om elektronisk kommunikation har Beredningen för rättsväsendets utveckling fått ett särskilt uppdrag (dir. 2003:145).

6.4.2 Aspekter på det internationella samarbetet

En egen fråga när internationellt informationssäkerhetsarbete diskuteras är hur svensk lagstiftning och arbetssätt påverkar det internationella samarbetet. För att kunna samarbeta effektivt på den internationella arenan förutsätts att Sverige åtnjuter förtroende och legitimitet hos sina internationella samarbetspartners. Vad beträffar de uppgifter som hänför sig till försvarssekretessen så skyddas dessa utifrån två säkerhetsskyddsnivåer – kvalificerat hemlig och hemlig. Internationellt finns det normalt fyra säkerhetsskyddsnivåer, t.ex. *top secret, secret, confidential* och *restricted* som används bl.a. inom EU-arbetet. Försvarsmakten har dock nyligen utkommit med en omarbetad version av Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd i syfte att skapa ett mer balanserat och internationellt anpassat skydd med fyra informationssäkerhetsklasser.

Utredningen har under arbetet gjorts uppmärksam på att skillnaden mellan den svenska och den internationella säkerhetsskyddsklass-

ningen kan ha lett till att Sverige har haft en högre skyddsnivå på vissa dokument än vad det internationella samarbetet erfordrar. Å andra sidan omfattas uppgifter som inte rör rikets säkerhet inte av säkerhetsskyddslagen. I det internationella samarbetet kan det faktum att det i vissa fall inte finns någon skyldighet i Sverige att hantera en handling som i ett annat land är sekretesskyddad i enlighet med säkerhetsskyddslagstiftningen komplicera samarbetet.

Även i den brottsförebyggande och lagförande verksamheten är det internationella perspektivet av stor vikt. Brottstypen är gränslös och gärningsmannen kan befinna sig i ett annat land än det land där effekterna av brottet visar sig. Internationellt samarbete är därför många gånger avgörande för möjligheten att eftersöka och lagföra gärningsmannen. De uppgifter som i många fall efterfrågas är uppgifter om trafikdata, vilket innebär att ett effektivt samarbete kräver viss harmonisering av lagringstider på det internationella planet. I detta sammanhang är även Cyberbrottskonventionen av stort intresse.

6.4.3 Särskilda frågor rörande samverkan med näringslivet

Företagen får i skilda sammanhang låta myndigheter ta del av uppgifter som hos företagen har ett högt sekretessvärde. Även om myndigheterna uppmärksammas på att uppgifterna är hemliga enligt lagen om företagshemligheter, är det inte säkert att myndigheterna bedömer att uppgifterna omfattas av sekretess enligt sekretesslagen. Även om uppgifterna skulle anses underkastade sekretess, kan denna få vika vid en sådan intresseavvägning som normalt förekommer enligt sekretesslagen. Företagen riskerar då att lida ett betydande förfång genom att konkurrenter och andra får del av vitala uppgifter om företagen. Att detta är ett problem visar sig genom företagens bristande villighet att rapportera om IT-incidenter eftersom dessa rapporter inte kan garanteras sekretess.

Detta problem har bl.a. uppmärksammats av Post- och telestyrelsen med anledning av inrättandet av funktionen för IT-incidentrapportering. I beskrivningen av en IT-incident kan ingå information om en organisations säkerhet i IT-system, t.ex. hur skyddet mot IT-incidenter är uppbyggt, vilka brandväggar som används, säkerhetsrutiner m.m. Även information om operativsystem och e-postsystem kan inrymmas. Denna information kan, om den

hamnar i orätta händer, användas för att t.ex. kartlägga nät och system, hitta angreppsvägar och tekniska sårbarheter.

Rapporter om IT-incidenter som lämnas till en myndighet (t.ex. Sitic-funktionen på Post- och telestyrelsen) blir allmänna handlingar enligt offentlighetsprincipen i och med att de inkommer till myndigheten. Då 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. Erfarenheterna från Sitic visar att näringslivets företrädare har visat ovilja mot incidentrapportering under hittills rådande förutsättningar.

Under 2002 lämnade Post- och telestyrelsen ett förslag till regeringen om modifiering av sekretesslagen, vars syfte vara att skapa förutsättningar för Sitic att sekretessbelägga incidentrapporter från i princip samtliga rapportörer, inte enbart från så kallade bevakningsmyndigheter. Justitiedepartementet bereder en proposition som kommer att lämnas till riksdagen under våren 2004. Utredningen återkommer i frågan efter att ha tagit del av propositionen.

Vid införandet av säkerhetsskyddslagen uttalade regeringen att det inte var aktuellt att utvidga säkerhetsskyddet så att det generellt omfattar också företagshemlig information som av en eller annan anledning görs tillgänglig hos myndigheter. I den utsträckning som näringslivets problem avser sekretesslagens utformning och myndigheternas tillämpning av denna, ansåg regeringen att dessa problem ligger utanför ramen för omfattningen av en säkerhetsskyddslag (prop. 1995/96:129 s. 25).

6.5 Kompetensförsörjning

6.5.1 Utbildning och forskning

Det finns, som utvecklats i kapitel 5, skäl att värdera behovet av särskilda insatser för en bred påverkan av attityder till informations- och IT-säkerhet, såväl beträffande informationssystem i arbetslivet som i hushållens ökade användning av dator- och IT-system. Främst gäller det att öka medvetenheten om sårbarhet och

risker, men också om metoder och åtgärder för att skapa säkrare system. Det finns också skäl att värdera behovet av enklare testhjälpmedel för att underlätta en förbättrad säkerhet. Frågor om informationssäkerhet är ledningsfrågor i näringsliv, myndigheter, kommuner och landsting. Det ställer stora krav på kompetens och på tillgång till kvalificerad utbildning.

Om säkerhetsmedvetande saknas hos de personer som hanterar hela eller delar av informationssystem är flertalet åtgärder för att skapa en rimlig säkerhetsnivå av begränsat värde. Det är därför nödvändigt med utbildning som bidrar till att utveckla säkerhetsmedvetandet. Sådana inslag bör finnas med från början redan i skolans grundläggande data- och IT-utbildning. Det gäller både på grundskole- och på gymnasienivå.

För högskolenivån avser utredningen att i det fortsatta arbetet belysa tillgången till säkerhetsinriktade ämnen inom bl.a. 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 t.ex. civilingenjörer, civilekonomer och i vissa andra akademiska examina.

Syftet bör i första hand vara att fördjupa säkerhetsmedvetandet men också att ge en grund för att lära känna administrativa och tekniska metodfrågor för sårbarhets- och riskanalys, utveckla beställarkompetens vid upphandling och inköp och utveckla ett kunnande inom säkerhetsområdet som är användbart i arbetslivet.

Utredningen kommer vidare att ägna uppmärksamhet åt mötet mellan teknik och juridik när det gäller informationssäkerhet. Detta kan kräva utvecklingsinsatser på olika nivåer. Utredningen avser att fördjupa analysen av behoven i denna del.

Behovet av kryptokompetens i samhället är stort och växande. Kompetenskraven har höjts kraftigt under senare år. Utredningen avser att återkomma med förslag till åtgärder för hur detta behov skall kunna tillgodoses.

Forskning behövs för att utveckla informationssäkerheten, både grundforskning och forskning om tillämpade metoder, ledningssystem och andra system, program och produkter. Den behövs också

för att utveckla kompetens och stimulera kvalitet i utbildningen. Det gäller både för den offentliga verksamheten och för näringslivet. Alla med sektorsansvar inom området informationssäkerhet måste känna ansvar för forskningen inom den egna sektorn.

Krisberedskapsmyndigheten har ett särskilt ansvar inom forskningsområdet att stimulera, initiera, beställa och delvis finansiera forskning rörande informationssäkerhet. Det gäller både forskning inom det allmänna universitets- och högskoleområdet och inom ramen för Försvarshögskolans och Totalförsvarets forskningsinstituts verksamhet. Detta ansvar kan behöva förtydligas ytterligare. Utredningen avser att skaffa sig en uppfattning om omfattning och inriktning på dagens forskning i informationssäkerhet och värdera behovet av ytterligare stimulans.

6.5.2 Kompetens hos beställare och leverantörer

Beställarkompetensen för informationssäkerhet är alltför svag, vilket är ett grundläggande problem. Ägarna av samhällskritisk infrastruktur måste först inse att den infrastruktur de äger är kritisk, att den behöver skyddas, att skyddet inte enbart skall vara fysiskt utan även ett informationssäkerhetsskydd. Om beställaren är medveten om vad som krävs av ett bra informationssäkerhetsskydd så är det också möjligt att definiera skyddet, anpassa det och upphandla.

Utredningen avser redovisa principer och överväganden om vilket ansvar samhället har för att utveckla beställarkompetens och former för en sådan kompetensutveckling.

Företeelsen outsourcing, att lägga verksamhet på entreprenad, ökar behovet av beställarkompetens. Under senare år har outsourcing av hela eller delar av informationstekniken till andra företag med specialkompetens blivit allt vanligare. Utredningen avser att belysa företeelsen som i många fall kan vara ett instrument för att till rimliga kostnader tillföra kompetens om informationssäkerhet och IT-system, samtidigt som det också kan medverka till att på längre sikt avhända myndigheter, kommuner eller företag grundläggande kompetens beträffande funktion och innehåll i IT-system och därigenom också informationssäkerhet. Beställarrollen behöver dock förtydligas även vid egen drift.

En metod att ytterligare utveckla beställarkompetens kan vara att använda en gemensam standard 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. En sådan standard är SS 62 77 99, Ledningssystem för informationssäkerhet, som har viss tillämpning internationellt. Den är även en ISO-standard sedan december 2000.

Utredningens avsikt är att värdera om en mera generell användning av informationsstandard är en bra och resurseffektiv metod för att utveckla beställarkompetens och skapa en höjd, tillika mera gemensam säkerhetsnivå 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.

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

Tillgång till certifierade program och produkter kan underlätta beställarrollen. Regeringen har uppdragit åt Försvarets materielverk att etablera en certifieringsfunktion för IT-säkerhet. Uppbyggnaden har av olika anledningar tagit tid. Ännu är exempelvis inga evalueringsföretag licensierade. Några certifikat har därigenom ännu inte heller kunnat utfärdas. Processen med uppbyggnad pågår dock. Utredningen avser att noga följs denna process som syftar till att underlätta upphandling av säkra produkter och system för myndigheter och andra beställare.

Utredningen har också till uppgift att följa verksamheten vid den teknikkompetensfunktion som etablerats vid Försvarets radioanstalt och den rikscentral för IT-incidentrapportering (Sitic) som etablerats vid Post- och telestyrelsen samt den funktion för om-

världsanalys som etablerats inom Krisberedskapsmyndigheten. Avsikten är att värdera behovet av och möjligheterna till kunskapsöverföring från dessa verksamheter till kompetenshöjande fortbildning inom främst myndigheter och andra med ansvar för samhällskritisk infrastruktur.

6.5.3 Tillsyn och revision

Den tillsyn och kontroll enligt Säkerhetsskyddslagen som Säkerhetspolisen och Försvarsmakten genomför inom sina respektive ansvarsområden har betydelse för att uppmärksamma och åtgärda brister i säkerhetsskydd.

2000-säkringen visade att revision är en konstruktiv metod för säkerhetsutveckling också inom området IT-säkerhet. Från och med 2004 gäller en ny revisionsstandard, RS 401, för revision i företag i datoriserad informationssystemmiljö. Den nya revisionsstandarden tillämpas ännu inte vid Riksrevisionens granskning av statliga myndigheter. Det är önskvärt att så snarast blir fallet.

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

6.6 Integrering av informationssäkerhet och signalskydd

Signalskydd är åtgärder som syftar till att förhindra obehörig insyn i och påverkan av elektronisk kommunikation. Ett viktigt medel för signalskydd är användning av kryptografiska funktioner. I signalskyddsbegreppet ingår även s.k. signalkontroll. Syftet med denna verksamhet är att kontrollera att gällande regelverk efterlevs och fungerar, att kontrollera att utrustningen fungerar på avsett sätt, och att kontrollera vilken information som riskerar att spridas till obehöriga i samband med känslig verksamhet.

Signalskyddet i Sverige har historiskt haft en stark koppling till totalförsvaret (se delbetänkande 1 om signalskydd). Behoven av att skydda information har varit helt knuten till sekretesslagstiftningen. Idag är behoven delvis annorlunda. Det finns ett behov av att

skydda information även om den inte är hemlig sett strikt med utgångspunkt i sekretesslagen. Signalskydd bör därför ses som ett medel för att åstadkomma en bättre informationssäkerhet och bör vara en naturlig del i informationssäkerhetsarbetet även utanför totalförvarsverksamheten.

Den tekniska utvecklingen inom informationssäkerhetsområdet visar också på detta genom att kryptografiska funktioner integreras i informationssäkerhetsprodukter. Detta innebär att signalskyddad informationshantering blir mer lättillgänglig för användarna. Det innebär också att kraven på verifiering av den kryptografiska funktionen blir alltmer framträdande liksom kraven att implementeringen av den kryptografiska funktionen sker på ett korrekt sätt. Säkra metoder för framtagning/generering och hantering av kryptonycklar är en annan viktig del av signalskyddet. Erfarenheter visar att en stor svaghet i användning av kryptosystem är just hantering och generering av kryptonycklar. Det är därför viktigt att det finns en fungerande signalskyddsorganisation med utbildad personal vid de myndigheter, m.fl. som använder signalskyddssystem.

Idag hanteras nämnda uppgifter av Totalförsvarets signalskyddssamordning (TSA) och Totalförsvarets signalskyddsskola (TSS) inom Försvarsmakten och tjänsterna avropas främst av totalförsvarsmyndigheter och för försvarsindustrins behov. En tydlig trend är att civila myndigheter m.fl. i allt större omfattning begär stöd med ovanstående uppgifter 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. Ett alltmer ökande behov av deltagande och stöd till internationella organisationers kryptoverksamhet har under senare tid vuxit fram. Det är i dessa sammanhang viktigt att det inom landet finns en kvalificerad resurs som kan tillhandahålla tjänster såsom granskning och i tillämpliga fall kryptogodkännande av svensktillverkade kryptoprodukter för internationella organisationers behov. Även för IT-säkerhetsprodukter utan uppenbara kryptologiska funktioner kommer nationell granskning och ett nationellt godkännande att krävas för att svensk industri skall kunna hävda sig internationellt. Uppgiften att godkänna kryptosystem för skydd av information som omfattas av sekretess eller annars är skyddsvärd bedöms öka i framtiden. För svensk kryptoindustris möjligheter att kunna erbju-

da kryptoprodukter till inter-nationella organisationer där nationellt godkännande krävs, är det särskilt viktigt att en nationell funktion för kryptogodkännande tydliggörs.

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

Det är viktigt att det finns ett entydigt regelverk för signalskyddet inom den offentliga förvaltningen. Regelverket skall ge ett stöd till dem som är ansvariga för informationssäkerheten vid respektive myndighet, organisation, etc. Det är också viktigt att det finns en central organisation som kvalitetssäkrar de systemprodukter, som regelverket förordar. De systemprodukter som finns på marknaden håller inte alltid tillräcklig kvalitet. Det krävs också en ständig uppföljning av produkterna. Samtidigt är det viktigt att behoven hos användarna styr vilka systemprodukter som skall kvalitetssäkras, eller i vissa fall utvecklas. Utredningen anser idag att det är en allt för stor eftersläpning mellan när behov av system med kryptografiska funktioner identifieras, tills de de facto finns i drift. En orsak till detta är att signalskyddsbehovet inte tas med i beaktande när informationssystemen utvecklas.

En annan orsak till att det sker en eftersläpning av signalskyddsfrågorna är den organisatoriska placeringen av ansvaret för dessa frågor. Idag är det Försvarsmakten som har samordningsansvaret inom Totalförsvaret. Det gör att avvägningen mellan Totalförsvarets signalskyddsbehov ställs mot Försvarsmaktens övriga behov av resurser, eftersom det idag inte finns några särskilt avsatta medel för denna verksamhet. Utredningen anser att det är viktigt att Sveriges anseende inom detta område kan upprätthållas genom väl avvägda satsningar. Det är därför viktigt att hänsyn tas till alla intressenter genom en aktiv dialog. Utredningen kommer att följa dessa frågor.

6.7 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.

Under de senaste åren har informationssäkerhetsfrågorna varit föremål för ett intensivt internationellt samarbete, bl.a. i form av förhandlingar samt utbyte av information och erfarenheter. En omfattande rese- och besöksverksamhet har genomförts. Utbytet har i många fall skett utan någon mer ingående nationell samordning. Även inom informationssäkerhetsområdet är det i många fall av väsentlig betydelse att hänsyn tas till överordnade svenska intressen, och att utgångspunkten för vårt internationella agerande utgörs av en gemensam svensk ståndpunkt. Utan en sådan samordning kan svenska representanter komma att framföra olika ståndpunkter som får till följd att målen inte uppnås och att samverkande nationer uppfattar Sverige som mindre seriöst. Det är utredningens uppfattning att det budskap som framförts i internationella sammanhang inte i alla lägen varit samordnat och därmed inte gynnat svenska intressen i den utsträckning som annars hade varit möjlig. Orsaken till detta kan vara den snabba utvecklingen inom området. På kort tid har informationssäkerhetsfrågorna uppmärksammats inom en rad internationella organisationer och politikområden. Vidare har den strategiska inriktningen på politiken i vissa avseenden inte varit tillräcklig för att ge vägledning i tillräcklig omfattning. Frågorna har behandlats inom vitt skilda politikområden, ibland med tydliga målkonflikter, vilket har gjort det svårt att skapa en gemensam värdegrund att utgå ifrån. En annan orsak kan vara uppdelningen av ansvaret inom informationssäkerhetsområdet, i meningen att det finns risk att samordningen har försvårats eller i vissa fall fallit mellan stolarna. Det krävs enligt utredningen inte några nya formella processer exklusivt för samordning i internationella sammanhang. Regeringskansliet har enligt sin instruktion ansvaret för att utse Sveriges ombud och andra representanter vid förhandlingar med annan stat eller vid förhandlingar med och mö-

ten inom internationella organisationer. Med en väl genomarbetad och förankrad nationell strategi och en tydlig arbetsfördelning inom Regeringskansliet och mellan myndigheterna bör de befintliga verktygen, dvs. gemensam beredning, regleringsbrev och myndighetsinstruktioner, vara tillräckliga för att hantera såväl förutsedda som snabbt uppkomna frågor. Det kan däremot finnas skäl att lägga större vikt vid de internationella frågorna när myndigheternas instruktioner och regleringsbrev ses över.

6.8 Finansieringsaspekter

En tillräcklig informationssäkerhet är en förutsättning för att infrastruktur, nätverk och system skall kunna utnyttjas på avsett sätt. Säkerheten gör också att nya tjänster kan skapas, såsom skett med t.ex. banktjänster via Internet och möjligheten att deklarera över Internet. Vidare är 24-timmarskonceptet baserat på flera kvalitativa tjänster till medborgarna till lägre kostnader. Säkerheten måste därför också ses som intäktsskapande eller kostnadsbesparande.

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.

Kostnader som föranleds av åtgärder för att öka informationssäkerheten kommer att drabba både de privata och offentliga sektorerna. Kostnaderna, alternativt de negativa effekterna, riskerar dock enligt utredningens bedömning bli avsevärt större om inga åtgärder vidtas. Vilka åtgärder som bör vidtas är en avvägning mellan kostnader för ökad säkerhet gentemot vinster i form av t.ex. minskad sårbarhet och säkrad kritisk information etc. Det är angeläget att metoderna för att göra denna typ av bedömningar används och utvecklas. Särskilt kan det gälla inom den offentliga sektorn där förtroendeförluster kan vara mer kännbara än ekonomiska förluster.

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.

Vissa åtgärder kan eventuellt samfinansieras mellan offentlig och privat sektor. Uppföljning av både verksamhet och kostnader i syfte att förbättra informationssäkerheten är också av betydelse. För att markera ambitionerna inom informationssäkerhetsområdet, kan det eventuellt behöva övervägas om några särskilda medel bör tillskjutas initialt.

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

6.9 Utgångspunkter för en nationell informationssäkerhetsstrategi

Enligt utredningen bör en nationell informationssäkerhetsstrategi ha ett långsiktigt framåtblickande perspektiv som kan ligga till grund för handlingsplaner och åtgärder på två till tre års sikt. Strategin vänder sig till myndigheter, näringsliv och organisationer, men även till enskilda användare, då de flesta idag är anslutna till olika lokala, nationella eller internationella informationstjänster. I de följande redovisar utredningen några utgångspunkter som bör 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 kan sammanfattas 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.

2002 publicerade OECD ”riktlinjer för säkerhet i informationssystem och nätverk” (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). I detta dokument lanserades begreppet ”säkerhetskultur” i samband med användandet av informationsteknik och användandet av Internet. Den svenska strategin skall enligt utredningen utvecklas med hjälp av OECD:s riktlinjer och skapa förutsättningar för en sådan säkerhetskultur.

En ökad medvetenhet om informationssäkerhet hos alla, även hos den enskilde individen, kommer att bidra till ett ökat och tryggare användande av nättjänster. Detta kommer också att positivt medverka till arbetet med att säkra samhällets kritiska infrastrukturer. Informationssäkerheten bidrar till det skydd och de rättigheter som medborgarna skall ha.

Akronymlista

BID	Bankernas id-tjänst
BITS	Basnivå för IT-säkerhet
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BRU	Beredningen för rättsväsendets utveckling
BSI	Bundesamt för Sicherhet in der Infromtionstechnik
BSS	British Security Service
BTH	Blekinge Tekniska Högskola
CAPC	Civil Aviation Planning COmmittee
CCPC	Civil Communication Planning Committee
CCRA	Common Criteria Recognition Arrangement
CEP	Civil Emergency Planning
CERT	Computer Emergency Response Team
CESG	Communications-Electronics Security Group
CIP	Critical infrastructure protection
CIIP	Critical information infrastructure protection
CIOS	Centrum för informationsoperationsstudier (FHS)
CIV	Civila enheten (Fö)
COTS	Commercial off-the-shelf
CPC	Civil Protection Committee
CSIA	Central Sponsor for Information Assurance
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Defence
DCSSI	Direction centrale de la sécurité des systèmes d'information
DNS	Domännamnssystem
DNSSEC	DNS Security Extensions
DNO	Datornätverksoperationer
EGC	European Government CERT Group
EkomL	Lagen om elektronisk kommunikation
ENISA	Europeiska nät- och informationssäkerhetsbyrån

ENUM	Nummersättning av IP-telefoni
EPS	Enheten för ekonomi, personal och samordning (Fö)
EG	Europeiska gemenskapen
EU	Europeiska Unionen
EUMS	Europeiska unionens militära stab
EWPITC	European Working Party on Information Technology Crime
FAPC	Food and Agriculture Planning Committee
FBI	Federal Bureau of Investigation
FESA	Forum of European Supervisory Authorities for Electronic Signatures
FFS	Försvarets författningssamling
FHL	Lagen om skydd av företagshemligheter
FHS	Försvarshögskolan
FM	Försvarsmakten
FMV	Försvarets materielverk
FN	Förenta Nationerna
FO/E	Forsvarets etterretningstjeneste
FOI	Totalförsvarets forskningsinstitut
FortV	Fortifikationsverket
FRA	Försvarets radioanstalt
Fö	Försvarsdepartementet
GAC	Governmental Advisory Committee
GSHQ	Government Communications Headquarters
HKV	Högkvarteret
HPM	High Power Microwave
ICANN	The Internet Corporation for Assigned Names and Numbers
IDA	Interchange of Data between Administrations
IO	Informationsoperationer
IP	Internet Protocol
IPC	Industrial Planning Committee
IRI	Institutet för rättsinformatik (Stockholms universitet)
ISAC	Information Sharing and Analyses Center
ISO	International Organisation for Standardisation
ISP	Inspektionen för strategiska produkter
IT	Informationsteknik
ITSA	Informationssäkerhetsavdelningen
IW	Informationskrigföring
JsyCC	Joint Systems Coordination Centre

KBM	Krisberedskapsmyndigheten
KBV	Kustbevakningen
KRI	Krigsförbandsledningen
LIS	Ledningssystem för informationssäkerhet
LAN	Local Area Network
MUST	Militära underrättelse- och säkerhetstjänsten
NACOSA	Nato CIS Operating and Support Agency
NATO	North Atlantic Treaty Organisation
NC3A	Nato Consultation, Command and Control Agency
NCSA	National Communications Security Authority
NDA	National Distribution Authority
NHTCU	National Hi-Tech Crime Unit
NISCC	National Infrastructure Security Coordination Centre
NSD	Näringslivets säkerhetsdelegation
NSi	Nationell samverkan för informationssäkerhet
NSM	Nasjonal Sikkerhetsmyndighet
OECD	Organisation on Economic Cooperation and Development
PBIST	Planning Board of Inland Surface Transportation
PBOS	Planning Board of Ocean Shipping
PC	Personal computer
PKI	Public Key Infrastructure
PfP	Partnerskap för fred
PST	Politiets sikkerhetstjeneste
PTS	Post- och telestyrelsen
RK	Regeringskansliet
RPS	Rikspolisstyrelsen
SACG	Swedish Anticounterfighting Group
SCEPC	Senior Civil Emergency Planning Committee
SekrL	Sekretesslagen
SGDN	Secrétariat Général de la Deéfense Nationale
SHS	Spridnings- och hämtningssystem
SIS	Senter for informationssikring
SIS	Standardiseringen i Sverige
SN	Statens Signalskyddsnämnd
SNITS	Informationssäkerhetsnätverket
SNS	Statens Signalskyddsnämnds skola
SOU	Statens offentliga utredningar
StabSbS	Stabs- och sambandsskolan
STUDS	Större utbrott av smittsamma djursjukdomar

SWEDAC	Styrelsen för ackreditering och teknisk kontroll
SÄPO	Säkerhetspolisen
TAK	Totalförsvarets aktiva kort
TSA	Totalförsvarets signalskyddsavdelning
TSS	Totalförsvarets signalskyddsskola
UD	Utrikesdepartementet
UD-SSSB	Enheten för säkerhet, sekretess och beredskap (UD)
UNIRAS	Unified Incident Reporting and Alert Scheme
VDI	Varslingssystem for Digital Infrastruktur
VINNOVA	Verket för innovationssystem
WAN	Wide Area Network
WARP	Warning, Advice and Reporting Points

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 informationssäkerhetsarbetet bör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informations säkerhetsområdet 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)

Statens offentliga utredningar 2004

Kronologisk förteckning

1. Ett nationellt program om personsäkerhet. Ju.
2. Vem tjänar på att arbeta? Bilaga 14 till Långtidsutredningen 2003/04. Fi.
3. Tvång och förändring. Rättssäkerhet, vårdens innehåll och eftervård. + Bilagor. S.
4. Förnybara fordonsbränslen. Nationellt mål för 2005 och hur tillgängligheten av dessa bränslen kan ökas. M.
5. Från klassificering till urval. En översyn av Totalförsvarets pliktverk. Fö.
6. Översyn av personuppgiftslagen. Ju.
7. Ledningsrätt. Ju.
8. Folkbildning och lärande med ITK-stöd – en antologi om flexibelt lärande i folkhögskolor och studieförbund. U.
9. Bokpriskommissionens fjärde delrapport. Det skall vara billigt att köpa böcker och tidskrifter IV. Ku.
10. Rätten till skadestånd enligt konkurrenslagen. N.
11. Sveriges ekonomi – utsikter till 2020. Bilaga 1–2 till Långtidsutredningen 2003/04. Fi.
12. Patientskadelagen och läkemedelsförsäkringen – en översyn. S.
13. Samhällets insatser mot hiv/STI – att möta förändring. S.
14. Det ofullständiga pusslet. Behovet av att utveckla den ekonomiska styrningen och samordningen när det gäller länsstyrelserna. Fi.
15. Tolkförmedling. Kvalitet registrering tillsyn. Ju.
16. Digital Radio. Ku.
17. Turistfrämjande för ökad tillväxt. N.
18. Brottsförebyggande kunskapsutveckling. Ju.
19. Långtidsutredningen 2003/04. Fi.
20. Genetik, integritet och etik. S.
21. Egenförsörjning eller bidragsförsörjning? Invandrarna, arbetsmarknaden och välfärdsstaten. Ju.
22. Allmänhetens insyn i partiers och valkandidaters intäkter. Ju.
23. Från verksförordning till myndighetsförordning. Fi.
24. Utlandstjänstens villkor. Arbetsvillkor, ersättningssystem och skatteregler för statligt anställda under utlandsstationering. UD.
25. Informera om samhällets säkerhet. Fö.
26. Arbetstid vid vägtransporter – förslag till ny lag. N.
27. En Ny Doktorsutbildning – kraftsamling för excellens och tillväxt. U.
28. Hyressättning av vissa ändamålsbyggnader. Fi.
29. Tre vägar till den öppna högskolan. U.
30. Folkbildning i brytningstid – en utvärdering av studieförbund och folkhögskolor. U.
31. Flyktingskap och könsrelaterad förföljelse. UD.
32. Informationssäkerhet i Sverige och internationellt – en översikt. Fö.

Statens offentliga utredningar 2004

Systematisk förteckning

Miljödepartementet

Förnybara fordonsbränslen. Nationellt mål för 2005 och hur tillgängligheten av dessa bränslen kan ökas. [4]

Näringsdepartementet

Rätten till skadestånd enligt konkurrenslagen. [10]

Turistfrämjande för ökad tillväxt. [17]

Arbetstid vid vägtransporter – förslag till ny lag. [26]