Studierapport "Att påverka EU:s informations-säkerhetspolitik"

Tobias Jonason

KBM:s utbildningsserie 2008:4

KRISBEREDSKAPS MYNDIGHETEN

Studierapport "Att påverka EU:s informationssäkerhets-politik"

Tobias Jonason

Titel: Studierapport ”Att påverka EU:s informationssäkerhetspolitik”
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: KeWim Van Cappellen.

ISSN: 1652-3539
KBM:s dnr: 319/2008
Produktion: Jupiter Reklam AB

Skriften kan laddas ner från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

Innehållsförteckning

Förord **5**
Sammanfattning **7**
1 Inledning **9**
1.1 Bakgrund 9
1.2 Syfte 5 10
1.3 Målgrupp och avgränsning 10
1.4 Analyssteg 11
1.4.1 Utveckling av byggstenar för ett strategiskt agerande i EU 12
1.4.2 Kartläggning av EU:s informationssäkerhetspolitik och svenska viljeyttringar 13
1.4.3 Analys av beröringspunkter samt svenska påverkansmöjligheter 14
1.4.4 Slutsatser avseende påverkansmöjligheter 14
1.5 Material och andra ingångsvärden 15
1.5.1 Litteratur- och internetstudier 15
1.5.2 Intervjuserier 16
1.5.3 Interna workshops 16
1.6 Disposition och läsanvisning 16

2 Utgångspunkter för ett strategiskt agerande i EU **19**
2.1 Kriterier för att hantera frågor inom EU:s ram – vad? 19
2.2 Faser i EU:s beslutsprocess – när? 23
2.3 Metoder för att utöva inflytande – hur? 25
2.3.1 Utanför EU:s beslutsstruktur 25
2.3.1 Inom ramen för EU:s beslutsstruktur 26

3 EU:s informationssäkerhetspolitik **35**
3.1 Introduktion till EU 35
3.2 Introduktion till EU:s informationssäkerhetspolitik 37
3.3 Aktörer och ansvarsområden 37
3.3.1 Generaldirektoratet för informationssamhället och medier (GD InfSo) 38
3.3.2 Generaldirektoratet för rättvisa, frihet och säkerhet (GD JLS) 39
3.3.3 Generaldirektoratet för informationsteknik (GD DIGIT) 40
3.3.4 ENISA – Europeiska nätverks- och informations säkerhetsbyrån 41

4 Sveriges viljeyttringar inom informationssäkerhetsområdet 45
4.1 Introduktion till svenskt strategiarbete inom informationssäkerhetsområdet 45
4.2 Kartläggning av svenska viljeyttringar 47
4.2.1 Tekniska medel 49
4.2.2 Normering 48
4.2.3 Ökad robusthet 48
4.2.4 Samverkan 48
4.2.5 Hantera incidenter 49
4.2.6 Kompetens 49

5 Att påverka EU:s informationssäkerhetspolitik 51
5.1 i2010 – EU:s strategiska ramverk för IKT-området 51
5.2 Svenska viljeyttringar inom ramen för EU:s informationssäkerhetspolitik 55
5.2.1 Tekniska medel 55
5.2.2 Normering 62
5.2.3 Ökad robusthet 69
5.2.4 Samverkan 70
5.2.5 Hantera incidenter 74
5.2.6 Kompetens 75

6 Slutsatser och åtgärdsförslag 83
6.1 Påverkansmöjligheter 84
6.2 Åtgärdsförslag 86

Källförteckning 93

Bilaga 1 – Kartläggning av svenska viljeyttringar 97

Bilaga 2 – Definitioner 101

Bilaga 3 – Statliga aktörer 103

Förord

I takt med att samhället i allt högre utsträckning förlitar sig på informations- och kommunikationsteknologier har informationssäkerhet blivit en allt viktigare fråga både på nationell och internationell nivå.

För att stödja och underlätta det svenska informationssäkerhetsarbetet i och gentemot EU har krisberedskapsmyndigheten (KBM) initierat studier där EU:s informationssäkerhetsarbete har utvärderats utifrån olika perspektiv. Under 2005 och 2006 genomförde Totalförsvarets forskningsinstitut (FOI) en kartläggning av de olika informationssäkerhetsaktörerna inom EU på uppdrag av KBM. Uppdraget följdes 2007 av en ny beställning med syftet att utveckla ett embryo till en strategi för hur Sverige skall agera för att uppnå ett större inflytande över EU:s informationssäkerhetspolitik. Resultat av studien återfinns i denna rapport.

För att sprida resultatet bland svenska aktörer anordnade KBM ett seminarium där projektgruppens slutsatser redovisades. Vid seminariet deltog representanter från Regeringskansliet, myndigheter och näringslivet med ansvar för informationssäkerhetsfrågor. Under den efterföljande diskussionen utrycktes farhågan att ett aktivt deltagande i EU:s informationssäkerhetsarbete kräver mycket energi och arbete och då i synnerhet om aktören ifråga inte besitter tillräcklig kunskap om EU:s struktur och beslutsprocesser. En annan aspekt som behandlades var det faktum att informationssäkerhetsfrågornas sektorövergripande

karaktär medför att de är utspridda på såväl civila som militära aktörer. Även om denna studie är avgränsad till KBM:s verksamhetsområde och den civila dimensionen av informationssäkerhetsområdet finns det således behov av informationsspridning mellan de båda dimensionerna för att skapa ett helhetsgrepp inför ett strategiarbete.

Studien har bedrivits i projektform med medarbetare från FOI Försvarsanalys. Projektet har utgjorts av Tobias Jonason (projektledare), Henrik Carlsen, Thomas Eneström (tidigare Jönsson) och Anna Utterström. Henrik Carlsen har framförallt bidragit med kompetens inom informationssäkerhetområdet medan Thomas Eneström och Anna Utterström främst arbetat med frågor kring EU:s beslutsprocesser. I detta arbete har även Helén Jarlsvik deltagit. Huvudförfattare till rapporten är Tobias Jonason. Projekt har kontinuerligt under arbetets genomförande fört en kontinuerlig dialog med projektmottagaren Linda Englund samt Per Oscarson på informationssäkerhetsenheten vid KBM.

TOBIAS JONASON
Projektledare

Sammanfattning

I arbetet med att förbättra det svenska samhällets informationssäkerhet är EU en självklar arena att förhålla sig till. Informations- och kommunikationsteknologier bedöms vara av stor vikt för unionens framtida utveckling och EU blir hela tiden mer aktivt på området. Det gäller även informationssäkerhet.

Syftet med studien har varit att analysera hur Sverige kan få större strategiskt inflytande när det gäller EU:s informationssäkerhet. Slutprodukten är ett förstadium till en strategi för påverkan som kan användas som källa till inspiration i framtida strategiarbete inom informationssäkerhetsområdet.

Studien har därför utvecklat byggstenar för ett strategiskt agerande i EU, kartlagt svenska viljeyttringar inom informationssäkerhetsområdet samt kartlagt EU:s informationssäkerhetsarbete. För att identifiera vilka verksamheter som är av svenskt intresse har sedan de svenska viljeyttringarna inom informationssäkerhetsområdet lagts som ett raster över EU:s arbete. Därefter kartlades de utvalda verksamheternas processer mer i detalj för att på så vis identifiera vilka möjligheter Sverige har att påverka dem.

Det finns stora möjligheter för Sverige att påverka EU:s informationssäkerhetsarbete. EU är idag en viktig arena när det gäller forskning, teknikutveckling samt lagstiftning och även till viss del mjukare styrmedel. I takt med att de informella kanalerna blivit allt viktigare när EU:s informationssäkerhetspolitik utformas, skapas ännu större förutsättningar att påverka inriktningen av EU:s informationssäkerhetsarbete genom aktivt och kunnigt agerande.

1 Inledning

1.1 Bakgrund

Tillgång till information har blivit alltmer självklart i dagens samhälle. Den utvecklade infrastrukturen för distribution av data samt förändrade livs- och beteendemönster har gjort att information finns tillgänglig på ett helt annat sätt än tidigare. Det är inte enbart individens privatliv som påverkas av att informations- och kommunikationsteknologier (IKT) används allt mer. Även en stor del av den dagliga verksamheten inom offentlig sektor och näringslivet bygger på IKT-system. Utvecklingen har fått ett sådant genomslag i samhället att IKT numera är ett kritiskt inslag i stora system inom traditionella industrier och samhällsviktiga verksamheter som kärnkraftverk, elektroniska kommunikationer, betalningssystem och vattenförsörjning. Samhällets ökade beroende av IKT medför att informationssäkerhetsområdet blir allt mer betydelsefullt. I USA varnar departementet för inrikes säkerhet (Department of Homeland Security) för att globaliseringen och det ökade beroendet av internet gör att risken för cyberattacker ökar. Samtidigt som antalet attacker ökar har antalet lagförda brott minskat, vilket tyder på att de som begår brotten har blivit allt skickligare och utnyttjar allt mer sofistikerade verktyg och metoder.

Informationssäkerhetsområdet är globalt till sin karaktär. Det gör att frågorna inte kan hanteras enbart inom rikets gränser. Sverige måste därför ta fram verktyg för att påverka utvecklingen inom IKT och informationssäkerhet såväl nationellt som internationellt. I detta sammanhang är Europa och EU ett viktigt forum för inflytande på utvecklingen inom informationssäkerhetsområdet. IKT-området är mycket viktigt för utvecklingen inom EU.

Kärnkraftverket Barsebäck i Skåne.
Konturen av byggnaderna syns i dimman.
Foto: Roland Bengtsson.

Mellan 2000 och 2004 stod sektorn för närmare 40 procent av tillväxten inom unionen.[1]

År 2006 gjorde FOI på uppdrag av KBM en kartläggning av EU:s informationssäkerhetsarbete.[2] Syftet var att förbättra Sveriges möjligheter att tillgodogöra sig resultaten av informationssäkerhetsarbetet. Kartläggningen visade att det finns stora möjligheter att påverka EU:s informationssäkerhetspolitik, men för att kunna utveckla det europeiska perspektivet och sedan konkret börja agera mer aktivt finns det ett behov av att identifiera hur Sverige kan bli en mer strategisk europeisk aktör. KBM beslöt därför att ta initiativ till en fortsättningsstudie, vars resultat redovisas i denna rapport.

1.2 Syfte

Syftet med studien har varit att analysera hur Sverige som nation kan få ett mer strategiskt inflytande på EU:s informationssäkerhetsarena. Resultatet av studien, i form av denna rapport, är inte en fullvärdig strategi utan ska snarare ses som ett förstadium till strategi – en idébank som kan användas som källa till inspiration i framtida strategiarbete inom informationssäkerhetsområdet.

1.3 Målgrupp och avgränsning

EU:s informationssäkerhetsarbete är mångsidigt till sin karaktär och hanteras i flera olika politikområden i EU:s tre s.k. pelare. Rapportens målgrupp är i första hand uppdragsgivaren KBM och därför ligger fokus på det EU-arbete som har den tydligaste kopplingen till KBM:s ansvarsområden. Detta innebär i praktiken att det i första hand är det informationssäkerhetsarbete som faller inom ramen för EU:s första pelare, den europeiska gemenskapen (EG) som uppmärksammas. Det arbete som bedrivs i den andra pelaren, den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den tredje pelaren, rättsliga frågor och inrikesfrågor (RIF) tonas därmed ned. Utöver att detta

[1] EU-kommissionens årliga rapport om den digitala ekonomin – I2010, 2nd annual report, IP/07/453 – Bryssel den 30 mars 2007.

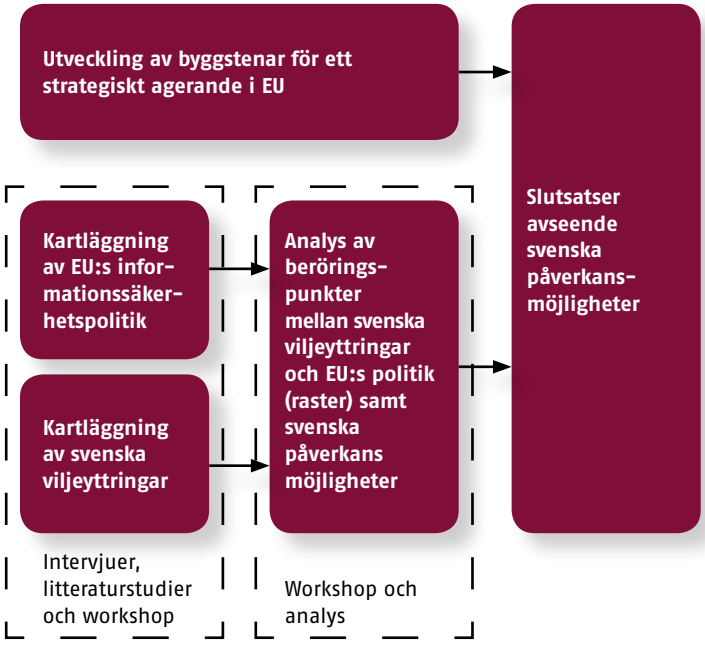
[2] Fylkner, Barck-Holst, Englund och Jarlsvik (2006), "Vem gör vad inom EU? – informationssäkerhetsfrågorna i fokus"

arbete inte är så relevant för KBM, vilar det på mellanstatlig grund. Det innebär att möjligheterna att påverk utvecklingen på ett mer detaljerat plan är begränsade. I den andra pelaren uppmärksammas dessutom informationssäkerhetsfrågorna uttalat endast undantagsvis, och i den tredje pelaren ligger tyngdpunkten i större utsträckning på operativt samarbete än på policyskapande. Även om rapporten på detta sätt har anpassats efter uppdragsgivaren KBM:s behov är den utformad på ett sådant sätt att vi bedömer att den är relevant även för andra myndigheter och departement som arbetar med informationssäkerhetsfrågor i svenska och europeiska sammanhang.

1.4 Analyssteg

Ordet "strategi" syftar vanligen på olika former av planer som gäller utveckling av verksamhet som helhet eller i avgränsade delar. En strategi har även en tidsaspekt och kortsiktiga, direkta framgångar tonas ofta ner till förmån för mål som gagnar verksamheten på längre sikt. Inom ramen för denna studie beskriver vi därför ett strategiskt inflytande som möjligheten att kunna påverka utvecklingen inom ett område eller process för att uppnå resultat som även på längre sikt är viktiga för Sverige.

För att skapa förutsättningar för ett strategiskt inflytande i EU krävs kunskap om när och hur Sverige ska agera. Man måste dock också ha kunskap om vilka områden – vad för typ av frågor – som är särskilt intressanta för Sverige. Det senare påverkas både av svenska viljeyttringar inom det aktuella sakområdet och hur lämpligt det är att hantera området inom EU:s ram, i motsats till att hantera det som en renodlad nationell angelägenhet eller i andra sammanhang där många länder är inblandade. De tre övergripande frågeställningarna när, hur och vad har genomsyrat studiearbetet. Frågorna återkommer både i våra generella resonemang om vad som är viktiga utgångspunkter för ett strategiskt agerande i EU, och i den specifika tillämpningen på EU:s informationssäkerhetsarbete. Studiearbetet har delats in i fyra analyssteg enligt schemat här nedan.



Figur 1: Arbetsprocess

1.4.1 Utveckling av byggstenar för ett strategiskt agerande i EU

I det första analyssteget utvecklade vi ett antal generella byggstenar som kan fungera som en utgångspunkt för ett strategiskt agerande i EU oavsett tillämpningsområde. Byggstenarna behandlar de tre övergripande frågorna för ett förstadium till en strategi för att påverka Sveriges agerande inom EU, utifrån frågorna vad, när och hur. Vad som bör ingå i en EU-strategi kan exempelvis fastställas med hjälp av olika kriterier för när det är lämpligt att hantera en fråga inom EU:s ram. Då ställer man det i motsats till att hantera den som en nationell angelägenhet eller inom andra multilaterala organisationer (svenska viljeyttringar, som är den andra dimensionen av frågan "vad?", hanteras i analyssteg 2). När Sverige bör agera inom EU kan fastställas med hjälp av en genomgång av faserna i EU:s beslutsprocess. Hur Sverige bör agera kan fastställas med hjälp av en genomgång av olika metoder för att utöva inflytande.

1.4.2 Kartläggning av EU:s informationssäkerhetspolitik och svenska viljeyttringar

I det andra analyssteget gjorde vi en kartläggning av EU:s informationssäkerhetspolitik och svenska viljeyttringar inom informationssäkerhetsområdet. Detta analyssteg bidrog därför till att belysa den andra dimensionen av frågan "vad?". Kriterier för när det är lämpligt att hantera en fråga inom EU:s ram, som vi hanterar i analyssteg 1, är den första dimensionen av frågan "vad?".

EU:s informationssäkerhetsarbete hade tidigare behandlats av FOI på uppdrag av KBM och redovisas i rapporten "Vem gör vad inom EU? – informationssäkerhetsfrågorna i fokus". Denna kartläggning av aktörerna och de viktigaste initiativen inom EU:s informationssäkerhetsarbete är utgångspunkten för studiens arbete.

Informationssäkerhetsarbetet inom EU är under ständig utveckling vilket gör att kartläggningar behöver uppdateras löpande. Studien uppdaterade kartläggningen enligt de mindre förändringar som har skett.

Vi ägnade mer tid åt att kartlägga svenska viljeyttringar inom informationssäkerhetsområdet. Eftersom området är sektorsöverskridande, hanteras ämnet ofta i olika forum av intressenter med skilda perspektiv. Sverige saknar en tydlig prioritering mellan sakfrågor, vilket gör att en informationssäkerhetsstrategi gentemot EU riskerar att omfatta ett alldeles för brett spektrum av sakfrågor. Resultatet blir att den blir alltför vag och verkanslös. För att ändå skapa en relation till det strategiska informationssäkerhetsarbete som har gjorts i Sverige under senare år. gjorde vi en kartläggning av svenska viljeyttringar utifrån de prioriteringar som åtminstone kan anas i bland annat informationssäkerhetsutredningen (SOU 2005:42 och SOU 2005:71), efterföljande proposition (2006:133) samt KBM:s lägesrapport 2007.[3] Det är inte upp till FOI att avgöra vilka specifika sakfrågor som är särskilt intressanta för Sverige. Däremot bedömer vi att en analys för att identifiera

[3] Referenser för spårbarhet återfinns i bilaga 1 – Kartläggning av svenska viljeyttringar.

prioriterade svenska viljeyttringar är ett fundamentalt moment för att kunna skapa en bas för ett svenskt strategiarbete inom informationssäkerhetsområdet. Eftersom studien dessutom endast ska resultera i ett förstadium till svensk strategi, finns det möjligheter att i ett senare skede se över valen av viljeyttringar.

1.4.3 Analys av beröringspunkter samt svenska påverkansmöjligheter

I det tredje analyssteget analyserade vi beröringspunkterna mellan EU:s informationssäkerhetspolitik och svenska viljeyttringar inom informationssäkerhetsområdet, som fanns med i kartläggningen i det andra analyssteget. De svenska viljeyttringarna lades som ett raster på EU:s informationssäkerhetspolitik och på detta sätt identifierades relevanta initiativ inom EU som berör de svenska viljeyttringarna. Varje svensk viljeyttring belystes med exempel. Eftersom EU:s informationssäkerhetsarbete är föränderligt och utvecklas över tiden uppmärksammades inte enbart det dagsaktuella läget, utan även tidigare genomförda processteg och initiativ.

Inom ramen för varje svensk viljeyttring (här finns viktiga frågor i kategorin "vad?") med tillhörande exempel på initiativ från EU:s informationssäkerhetsarbete, gjorde vi en analys av svenska möjligheter att påverka. Med det menar vi när och hur Sverige bör agera för att påverka EU inom det aktuella området. Som utgångspunkt för denna informationssäkerhetsspecifika analys använde vi de generella byggstenar som utvecklats i det första analyssteget.

1.4.4 Slutsatser avseende påverkansmöjligheter

I det fjärde och avslutande analyssteget – studiens syntesarbete – drog vi ett antal slutsatser av övergripande karaktär, samtidigt som vi lade fram förslag på mer konkreta åtgärder.

1.5 Material och andra ingångsvärden

För att kunna utföra de analyssteg som vi har beskrivit ovan, gjorde vi en faktainsamling genom litteratur- och internetstudier samt intervjuserier i både Sverige och EU. Andra viktiga ingångsvärden var två interna seminarier.

1.5.1 Litteratur- och internetstudier

Kartläggningen av EU:s informationssäkerhetspolitik är gjord utifrån tidigare svenska rapporter om EU:s informationssäkerhetsarbete samt offentligt material från svenska myndigheter och EU. Materialet från EU består till största delen av primärmaterial från EU:s institutioner och då särskilt från kommissionen och dess olika generaldirektorat. Materialet kan bestå av lagtexter, arbetsprogram, rapporter, utvärderingar och annat material som finns att tillgå på EU:s olika sidor på nätet. Eftersom ett förstadium till en påverkansstrategi omfattar alla aspekter av EU:s beslutsprocess utnyttjar vi material som tagits fram under beslutsprocessens samtliga faser.

Brottsförebyggande rådet. BRÅ presenterar den hitills största svenska studien av IT relaterad brottslighet. Foto: Fredrik Sandberg.

1.5.2 Intervjuserier

För att identifiera möjligheter och verktyg för att påverka EU:s informationspolitik räcker det inte alltid att bara använda offentligt material, särskilt med tanke på att den informella beslutsprocessen tenderar att få allt större betydelse för beslut inom informationssäkerhetsområdet. Vi har därför intervjuat deltagare i olika EU-initiativ som har betydelse för informationssäkerhetsområdet. Intervjuerna har gjorts både i Sverige och i andra EU-länder.

Intervjuserierna har framför allt fokuserat på vilka sakområden som intervjupersonens institution behandlar, hur processen utvecklar sig samt vilka möjligheter som finns att påverka informationssäkerhetsagendan i EU.

1.5.3 Interna seminarier

När vi arbetade med att kartlägga svenska viljeyttringar höll vi ett internt seminarium, vars resultat sammanfattas i bilaga 1. Ytterligare ett internt seminarium hölls med syfte att identifiera beröringspunkter, när de identifierade svenska viljeyttringarna lades som ett raster på EU:s informationssäkerhetspolitik.

1.6 Disposition och läsanvisning

I kapitel 2, "Utgångspunkter för ett strategiskt agerande i EU", presenterar vi de byggstenar som behandlar de tre övergripande frågorna vad, när och hur Sverige ska agera inom EU. Byggstenarna är generella till sin natur och kan användas närhelst ett strategiarbete inleds. Det aktuella kapitlet motsvarar resultatet av studiens första analyssteg.

I kapitel 3, "EU:s informationssäkerhetspolitik", och kapitel 4, "Svenska viljeyttringar inom informationssäkerhetsområdet", redovisar vi resultatet från studiens andra analyssteg. De båda kapitlen ger en empirisk bakgrund till vad som kan sägas utgöra viktiga informationssäkerhetsfrågor i EU och i Sverige. Läsare som är bekanta med innehållet i rapporten "Vem gör vad inom EU? – informationssäkerhetsfrågorna i fokus" kan hoppa över kapitel 3.

Kapitel 5, "Att påverka EU:s informationssäkerhetspolitik", är rapportens kärna. I detta kapitel, som är strukturerat utifrån svenska viljeyttringar (viktiga frågor i kategorin "vad?") presenterar vi resultatet från studiens tredje analyssteg där en analys görs av när och hur Sverige bör agera för att påverka EU inom det aktuella området.

Avslutningsvis, i kapitel 6, "Slutsatser och åtgärdsförslag", sammanfattar vi resultatet från studiens syntesarbete som är det fjärde analyssteget.

2 Utgångspunkter för ett strategiskt agerande i EU

I detta kapitel presenterar vi olika byggstenar som man kan använda för att skapa utgångspunkter för en svensk EU-strategi inom informationssäkerhetsområdet. Byggstenarnas grund är de tre tidigare presenterade frågeställningarna som är relevanta för vilket EU-strategiarbete som helst: Vad, när och hur ska Sverige agera för att utöva inflytande i EU? Inledningsvis redogör vi översiktligt för några kriterier som är viktiga att beakta vid en bedömning av vad som bör drivas inom EU:s ram, i stället för att kanske hanteras nationellt eller i andra forum där flera länder deltar. Därefter lägger vi en grund för att analysera när i tiden som det är lämpligt att agera i EU utifrån en beskrivning av de olika faserna i EU:s beslutsprocess. Avslutningsvis presenterar vi tänkbara metoder för hur inflytande inom EU kan uppnås.

2.1 Kriterier för att hantera frågor inom EU:s ram – vad?

Europeiska unionen är unik i förhållande till andra internationella organisationer, bland annat för att den är utrustad med alla de instrument som staten normalt sett förfogar över: lagstiftningsmakt, finansiella resurser och egen kunskapsgenererande kapacitet. På grund av det kan utvecklingen inom informationssäkerhetsområdet i stor utsträckning styras på nationell nivå såväl som på EU-nivå.

Innan frågan förs upp på EU-nivå bör dock en analys göras av huruvida EU är ett relevant forum i det enskilda fallet. Här finns det två avgörande faktorer: å ena sidan behovet av att känna till och anpassa styrmedlen efter nationella förhållanden och å andra sidan behovet av samordning med andra medlemsstater för att nå önskad effekt. Andra faktorer som är viktiga att beakta är hur konkurrensen påverkas och i vilken mån det behövs en

Justitia.

gemensam ståndpunkt för att påverka länder utanför EU. Nedan har vi ställt upp ett antal frågor för en överblick över vad man bör förhålla sig till när man bedömer om vägen via EU är den mest lämpliga. Frågorna ska betraktas som ett led i att identifiera vad eller vilka frågor som Sverige ska driva inom EU.

Är effektiviteten i åtgärden beroende av att andra länder vidtar åtgärder?

Om en fråga ska lyftas från nationell nivå bör detta tillföra ett mervärde. Denna princip uttrycks inom EU i den så kallade subsidiaritetsprincipen. Den innebär att EU ska vidta åtgärder endast om dessa är mer effektiva än de som kan vidtas på nationell, regional eller lokal nivå. Eftersom informationssystem i många fall är gränsöverskridande till sin karaktär är beroendet av andra länders agerande stort på informationssäkerhetsområdet.

Beroendet kan ta sig flera olika uttryck. Det kan handla om ett direkt fysiskt beroende som när anläggningar i andra länder kommer till skada och Sverige direkt blir lidande. Ett exempel på sådana anläggningar skulle kunna vara driftcentraler utomlands varifrån informationsnät i Sverige drivs. Beroendet kan också vara direkt logiskt. I detta fall skulle det kunna handla om brister i programvara eller kryptering tillverkad i andra länder som inverkar negativt på säkerheten i Sverige. Slutligen skulle det kunna röra sig om beroende genom uppkoppling. Ett exempel på det är när personer som fysiskt sett befinner sig utanför landets gränser hotar information eller informationssystem i Sverige via internet. Det krävs då att det går att lita på att även andra länder vidtar åtgärder för att förhindra it-brott och lagför dem som har orsakat skada på informationssystem i ett annat land.


Informationssystem hotas via internet.

Är det redan en EU-fråga?

En viktig aspekt som är lätt att förbise är om den aktuella frågan redan har förts upp på EU-nivå. Om det inte är så kan det vara rätt tidpunkt för ett initiativ, beroende på utvecklingen i övrigt. Om det å andra sidan redan är

en EU-fråga krävs det likväl engagemang och aktivitet i frågan på EU-nivå för att skapa förutsättningar för att processen ska leda i önskad riktning.

Det kan dock också vara viktigt att analysera i vilken utsträckning frågan borde ha blivit en EU-fråga, eftersom detta påverkar hur man agerar. Om man bedömer att en fråga uteslutande borde ha behandlats på ett nationellt plan eller i en annan internationell organisation, kan man försöka begränsa de åtgärder som vidtas inom EU.

Är lagstiftning lämpligt?

EU har en klar fördel gentemot andra organisationer (OECD, FN m.fl.) eftersom unionens överstatliga karaktär skapar möjligheter till gemensam lagstiftning. Sverige försöker dock generellt sett att undvika att ta till lagstiftning i första hand. I vissa fall, särskilt då aktörerna inte upplever något egenintresse av att reglera en fråga, kan dock andra styrmedel vara tandlösa. Om problemet dessutom är gränsöverskridande, framstår nog gemensam lagstiftning ofta som det enda sättet att effektivt komma tillrätta med problematiken. Inom informationssäkerhetsområdet är det inte ovanligt att gränsöverskridande problem kombineras med att självreglering saknas. Gemensam lagstiftning kan därför i många fall vara ett lämpligt styrmedel på detta område. Allra störst effekt får gemensam lagstiftning om den blir normbildande för hur frågorna hanteras globalt.

Det är viktigt att framhålla betydelsen av att tidigt utvärdera möjligheterna att få till stånd lagstiftning som är utformad ungefär enligt de önskemål man har. I vissa fall kanske processen tar en helt annan riktning än vad initiativtagaren hade tänkt sig. I slutändan kanske ingen lagstiftning alls på EU-nivå upplevs som ett bättre alternativ än det uppnådda resultatet.

Behövs gemensamma medel?

För att bekämpa hoten mot informationssystemen kan det krävas en mängd olika åtgärder, t.ex. att hämta in

underrättelser, att bekämpa brott och att utveckla den kunskap som finns.

Sverige är i detta sammanhang en liten nation med begränsade resurser och vissa projekt som vore värdefulla att genomföra blir aldrig av eftersom ingen vill ta på sig finansieringsansvaret. Då blir det särskilt viktigt med möjligheter till gemensam finansiering på EU-nivå. Generellt sett är Sveriges syn på gemensam finansiering ganska restriktiv. Det beror på att vi betalar in förhållandevis mycket till EU-budgeten. Men finansiering behöver inte ske genom att nya medel tillförs, utan även kan ske genom omfördelningar i budgeten.

Gemensamma medel kan också användas som en form av mjukt styrmedel. Genom att finansiera t.ex. projekt som tar sikte på att upplysa medborgarna om vikten av att vidta skyddsåtgärder när det gäller informationsteknisk utrustning, kan utvecklingen inom medlemsstaterna styras utan att man behöver ta till lagstiftning.

Behövs en gemensam position i förhållande till andra länder?

En stor del av it-hoten som t.ex. dataintrång har sitt ursprung i länder utanför EU. Sverige är ett välutvecklat it-land och bör därför vara särskilt intresserat av att länderna i fråga vidtar åtgärder mot dem som ligger bakom hoten. Samtidigt är det svårt för ett litet land som Sverige att lägga tillräcklig tyngd bakom argumenten för att kunna påverka. Då kan det vara mer ändamålsenligt att försöka få EU att utöva påtryckningar för att åtgärder ska vidtas, via sina samarbetsavtal med länder utanför unionen. Eftersom EU har någon form av avtal med de flesta länder i världen, exempelvis biståndS- och handelsavtal, kan det vara en effektiv metod.

Det krävas en mängd olika åtgärder för att hämta in underrättelser och bekämpa brott mot informationssystemen.

Idag finns redan generella klausuler i avtalen med tredje land som tar sikte på mänskliga rättigheter och bekämpandet av terrorism. I sitt meddelande om skräppost, spionprogram och sabotageprogram förklarade kommissionen att avsikten är att försöka se till att dessa tre problem

särskilt betonas i avtal med tredje land.[4] Förutsättningarna på informationssäkerhetsområdet skulle säkert kunna förbättras om det fördes in fler klausuler som tar sikte på informationssäkerhet i befintliga avtal.

Finns det risk för snedvriden konkurrens?

Den främsta anledningen till att EU skapade gemensamma regler som tog sikte på informationssäkerhet var inte att öka säkerheten i sig, utan att skapa goda förutsättningar för den inre marknaden och stärka EU:s konkurrenskraft gentemot övriga världen.[5] Det är alltså viktigt att förhålla sig till konkurrensfrågor för att kunna avgöra om en fråga bör lyftas till EU-nivån. Om man t.ex. gör bedömningen att säkerhetsstandarder används som dolda handelshinder kan det finnas skäl att undersöka om gemensam lagstiftning skulle kunna motverka detta.

2.2 Faser i EU:s beslutsprocess – när?

NÄR?

Om man ska kunna utöva inflytande inom EU måste man känna till EU:s beslutsprocess och de tre faser som den kan delas in i: initiativfasen, beslutsfasen och genomförandefasen. t sett kan vi säga att de aktörer som får möjlighet att utöva inflytande och de tillvägagångssätt som de använder varierar, beroende på vilken fas och vilket politikområde man befinner sig inom. Tyngdpunkten i översikten nedan ligger på hur beslutsprocessen är utformad inom ramen för EG-samarbetet, som en följd av de avgränsningar vi gjorde i det inledande kapitlet. Tanken är att detta avsnitt vara ett verktyg för att ta reda på när i tiden man bör agera för att i så stor utsträckning som möjligt kunna påverka arbetet framåt.[6]

Initiativfasen

Initiativfasen i EU:s beslutsprocess är ofta lång och omfattar alla de aktiviteter som leder fram till att ett förslag till ny

[4] KOM/2006/0688, skräppost, spionprogram och sabotageprogram.
[5] Jönsson & Jarlsvik (2005) Krisberedskapsmyndigheten och Europeiska unionen, s. 40.
[6] För en utförligare beskrivning av de olika faserna i EU:s beslutsprocess se Jönsson & Jarlsvik (2005) Krisberedskapsmyndigheten och Europeiska unionen.

lagstiftning eller ny politik presenteras. Det är kommissionen som har rätt att ta initiativ i denna fas. För att hämta synpunkter från olika aktörer och stärka förslagets legitimitet använder sig kommissionen av många olika metoder. Det handlar här bland annat om konferenser, expertmöten, seminarier och öppna möten för det särskilda ändamålet. Dessutom genomförs ofta så kallade öppna samråd via internet, där berörda aktörer kan kommentera kommissionens förslag. Efter att konsultationstiden har gått ut publiceras oftast alla bidrag eller en analys av resultaten.

Beslutsfasen

Beslutsfasen inleds då ett förslag till lagstiftning eller annat beslut har presenterats. I den första pelaren fattas de flesta beslut här med kvalificerad majoritet. Det är rådet och i många fall även parlamentet som tar ställning till förslagen. Rådet är medlemsstaternas forum i EU och arbetet bedrivs i huvudsak på tre olika nivåer. Förhandlingar inleds på tjänstemannanivå i tematiska rådsarbetsgrupper. Varje arbetsgrupp har en "ägare" eller ett ansvarigt departement som samordnar det förberedande arbetet. När arbetsgrupperna har diskuterat frågorna, behandlar de ständiga representanternas kommitté de frågor som kvarstår som olösta. Kommittén består av medlemsstaternas EU-ambassadörer. Slutligen fattas beslut på ministernivå av medlemsstaternas fackministrar.

Genomförandefasen

Genomförandefasen är i de flesta fall den längsta av de olika beslutsfaserna och i den deltar både kommissionen och medlemsstaterna. Ett syfte med arbetet i denna fas är att precisera lagstiftning som har förhandlats fram, genom att utforma mer konkreta regler och arbetsprogram. Ett annat är att aktivt utföra eller hämta in resultatet av politiken genom att t.ex. delta i forskning och ordna utbildningar. Det är kommissionen som leder arbetet i genomförandefasen, men medlemsstaterna har möjlighet att påverka politikens utformning genom de så kallade genomförandekommittéerna. Dessa måste godkänna kommissionens förslag till beslut.

2.3 Metoder för att utöva inflytande – hur?

Det finns så många alternativa tillvägagångssätt att det nästan är omöjligt att veta hur man ska agera för att nå inflytande i EU. Man måste med andra ord göra en grundlig analys av förutsättningarna i det enskilda fallet. Nedan har vi ändå ställt upp olika metoder som kan lägga grunden för en påverkansstrategi. Utgångspunkten är de intervjuer som vi har gjort inom ramen för studien, i analyser och material där politiskt inflytande diskuteras[7] samt i tidigare rapporter och utredningar som beskriver de karakteristiska dragen för informationssäkerhetsområdet.

Även om några av de metoder som vi beskriver nedan skulle kunna betraktas som viktigare än andra har vi inte graderat dem, eftersom de i stor utsträckning är beroende av varandra och knappast gör någon skillnad var och en för sig. Eftersom syftet med avsnittet är att utreda hur man kan få inflytande inom EU, fokuserar vi här nedan på hur man kan påverka processen framåt inom ramen för den ordinarie beslutsstrukturen. Men först beskriver vi översiktligt två tillvägagångssätt som kan användas för att utöva inflytande utanför EU:s beslutsstruktur.

2.3.1 Utanför EU:s beslutsstruktur

Vara en förebild

Ett sätt att utöva inflytande utanför den ordinarie beslutsstrukturen kan vara att genomföra åtgärder på hemmaplan för att kunna visa goda exempel och för att i ett senare skede kunna exportera ett väl fungerande arbetssätt. Kanske är detta särskilt viktigt inom informationssäkerhetsområdet där stater kommit olika långt i utvecklingen. Att driva en fråga med "hårdare" styrmedel kan då bli svårt. En stat som ännu bara skapat ett förstadium till en policy kanske anser att ännu ett steg i reglerande riktning är för stort, om den som förespråkar mer omfattande åtgärder inte kan visa ett framgångsrecept utan förödande fallgropar på vägen.

[7] Se särskilt Nilsson, Maria (2003) Europeisk säkerhets- och försvarspolitik – en studie om svenska möjligheter att påverka.

Rent konkret kan det här handla om att skapa olika arrangemang i form av t.ex. seminarier för att uppmärksamma en fråga. Förmodligen är det allra mest effektivt om arrangemanget ligger i nära anslutning till att frågan blir aktuell i den allmänna debatten. Då förstärks intrycket av att det är en central frågeställning som ligger rätt i tiden.

Påverka via andra organisationer

EU inspireras ganska ofta av andra aktörer då nya policyer och regelverk skapas. Av detta skäl kan det vara en god idé att påverka via andra framträdande organisationer på informationssäkerhetsområdet. Etablerade organisationer med gedigen kunskap inom en specifik fråga kan utan tvekan i många fall skapa ett större tryck än en enskild stat.

Informationssäkerhetsfrågor behandlas i flera internationella sammanhang. Sverige deltar i EU:s arbete, men även inom andra organisationer som t ex OECD som bland annat har tagit fram riktlinjer för säkerhet i informationssystem och nät. Det är därför inte självklart att det är effektivare att driva en fråga inom EU-strukturen.

Om man bedömer att en fråga bäst behandlas inom ramen för ett annat forum än EU kan det aktiva deltagandet där även vara en strategi i sig. Genom att tillföra mer information och kunskap till en annan aktör, kan man bidra till att denna får större tyngd på den politiska arenan. För en liten stat som Sverige är en sådan strategi emellertid beroende av att koalitioner byggs.

2.3.1 Inom ramen för EU:s beslutsstruktur

Kunskap

Kunskap

Förberedelserna inför behandlingen av en fråga och den mer långsiktiga kompetensuppbyggnaden har avgörande betydelse för hur en framgångsrik en strategi blir. Utan gedigen kunskap och kompetens vid förhandlingsbordet kommer möjligheterna att utöva inflytande att bli betydligt mindre.

Kunskap skulle kunna delas in i tre block: kunskap om sakfrågor och övergripande frågor, kunskap om andra aktörers inställning samt kunskap om själva processen och hur man agerar i de olika faserna av den.

När det gäller sakfrågor behövs det både bred och djup kunskap. Den breda kunskapen är viktig för att olika frågor och processer ofta är kopplade till varandra. Även om en del processer inte verkar direkt beröra det egna ansvarsområdet kan det därför vara viktigt i ett senare skede att ha övergripande kunskaper. Att inför en förhandling endast ha inblick i den enskilda sakfrågan minskar förmågan att argumentera för den egna ståndpunkten. Argumenten styrs ju ofta av övergripande målsättningar och förhållandet till utvecklingen i övrigt. Inom informationssäkerhetsområdet är det också viktigt att ha bred kunskap för att frågornas spridning på olika aktörer annars kan bidra till duplicering. De djupare kunskaperna å andra sidan är en förutsättning för att kunna presentera förslag som för processen framåt. Utan dessa hamnar tyngdpunkten i arbetet i stället på att skapa en överblick och vidarebefordra information hemåt.

För att framgångsrikt kunna argumentera i en fråga måste man känna till andra medlemsstaters syn på utvecklingen i olika frågor och processer, men också hur kommissionen och näringslivet ser på utvecklingen. Dels bidrar detta till att förutse utvecklingen och i tid skapa motargument, dels kan härigenom möjliga samarbetspartner identifieras.

På ett område som informationssäkerhet blir det särskilt tydligt att processkunskap, det tredje kunskapsblocket, har stor betydelse. Det beror på att arbetet i stor utsträckning är nätverksbaserat. Beslutsprocessen är komplex, särskilt när det gäller mängden aktörer och blandningen av privata och offentliga konstellationer. Det understryker behovet av djupare kunskaper om processerna som aktörerna verkar i. Man bör därför tidigt ta upp frågor som hur processen ser ut i olika beslutsfaser och när möjligheterna är som störst att utöva inflytande.

Aktivt engagemang

Aktivt engagemang

Att vara aktiv i en process innebär inte bara att vara synlig i den meningen att man deltar i processen. Man måste också signalera avsikter och tydligt ta ansvar för att föra processen framåt.

Inom en nätverksbaserad struktur som i stor utsträckning är baserad på informella kontakter kommer starka, kunniga och handlingskraftiga individer att vara en av de grundläggande förutsättningarna för ett aktivt engagemang. Det krävs ofta att dessa på egen hand skaffar sig relevanta informationskanaler. Utan rätt informationskanaler blir det omöjligt att följa utvecklingen och bedöma om ett initiativ ligger rätt i tiden.

Det är också av central betydelse att vara aktiv i processen som sådan, inte bara att driva specifika sakfrågor. Därmed kan man få respekt och styra utvecklingen i en gynnsam riktning. Det handlar t.ex. om att ha representanter högre upp i strukturerna och att på olika sätt agera drivande och skapa kompromisslösningar.[8] Att vara aktiv i processen är vidare en förutsättning för att kunna driva olika sakfrågor. Det beror bland annat på att frågor ganska ofta fastnar på lägre nivåer. Det blir svårt att driva en linje utan processvana och förutsättningar att föra upp frågorna till nivån ovanför. Slutligen är det viktigt att inte bara reagera på befintliga förslag utan att även att agera i god tid och i takt med utvecklingen. För den aktör som vill påverka utformningen av EU:s krisberedskapsarbete är det särskilt viktigt att agera och klargöra sin ståndpunkt i initiativfasen. Det beror dels på att det kan vara svårt att påverka de större dragen i processen i ett senare skede, dels på att trovärdigheten kan urholkas då en aktör i ett senare skede ställer sig negativ till ett förslag som den tidigare inte haft några invändningar emot.

[8] Nilsson, Maria (2003) Europeisk säkerhets- och försvarspolitik – en studie om svenska möjligheter att påverka, s. 34.

Prioriteringsförmåga

Prioriteringsförmåga

För att kunna vara aktiv och synlig på informationssäkerhetsområdet måste man ha god förmåga att prioritera. Att det finns så många olika aktörer och frågor inom detta område gör det omöjligt att utveckla ståndpunkter i alla frågor.

Med andra ord måste Sverige kunna prioritera, för att i egenskap av småstat kunna nå konkreta mål. Om prioriteringarna är tydliga kan svenska representanter dels överblicka processer och rapportera hemåt, dels vara aktiva och synliga i arbetet framåt. Det signalerar i sin tur handlingskraft och förmåga att satsa politiskt. För övriga aktörer blir det då tydligt hur Sverige vill profilera sig och det blir lättare för eventuella koalitionspartner att ge sig tillkänna. Överhuvudtaget bidrar nog en god prioriteringsförmåga till att andra får intryck av att Sverige är en stat att räkna med. Detta är av central betydelse i en nätverksbaserad process där aktörer bara tar informella kontakter med de stater som visar drivkraft.

Koalitionsbyggande

Koalitionsbyggande

En liten stat som Sverige är i större utsträckning än större medlemsstater beroende av att så tidigt som möjligt i processen skapa koalitioner med andra medlemsstater eller ansluta sig till befintliga koalitioner för att kunna utöva inflytande. För att framgångsrikt kunna bygga allianser krävs det att den linje som förs är sammanhängande och har tyngd. Det kan därför vara fördelaktigt med långsiktiga samarbeten, dels för att förutsägbarheten gör det enklare för ytterligare stater att ansluta sig i ett senare skede, dels för att linjen hinner "rota sig". Vi vill också framhålla att det på informationssäkerhetsområdet är särskilt viktigt att bygga upp relationen med näringslivets aktörer och skapa kanaler till dessa.

"Personliga kontakter och regelbunden kommunikation med andra medlemsstater har blivit allt viktigare."

På informationssäkerhetsområdet är kvalificerad majoritetsröstning huvudregeln. Då blir koalitionsbyggande ännu viktigare, eftersom möjligheten att blockera ett visst beslut inte finns. Antalet koalitionspartner har också blivit fler eftersom unionen har utvidgats. Personliga kontakter och regelbunden kommunikation med andra medlemsstater har blivit allt viktigare. Genom kommunikation och informationsutbyte skapas det en klarare uppfattning om vilka stater som kan tänkas inta en liknande ståndpunkt, men också om vilka stater som vill driva en linje som står i strid med den egna.

Koalitioner har alltså huvudsakligen två funktioner. Dels är syftet att förvalta och driva fram egna linjer, dels handlar det om att mota bort ståndpunkter som leder utvecklingen i en ofördelaktig riktning. Det kan man göra antingen genom att gemensamt motsätta sig ett befintligt förslag eller genom att föra fram nya.

Argumentationsförmåga

Argumentationsförmåga

Då en aktör har kommit långt inom ett område, som Sverige torde göra inom informationssäkerhetsområdet, är det avgörande att aktören kan visa fördelarna med den egna policyn för att övertyga de länder som behöver omfattande åtgärder och resurser för att uppnå en godtagbar standard. Hur ett förslag formuleras kan här vara av central betydelse för den framtida processen. Hur viktig argumentationen är i det enskilda fallet beror dock troligen på frågans karaktär. Om det handlar om en fråga där stormakterna i princip redan har bestämt sig väger förmodligen motargument från en mindre stat inte särskilt tungt. Handlar det i stället om en situation där ny politik ska skapas är situationen en annan.[9]

Att presentera nyttan för gemenskapen snarare än för den enskilda nationen är ett sätt att nå framgång i argumentationen. Det handlar här om att förmedla en bild av att man ser till det europeiska intresset och allas bästa. Om det inte är möjligt är det i många fall bättre att föra fram

[9] Nilsson, Maria, (2003) Europeisk säkerhets- och försvarspolitik – en studie om svenska möjligheter att påverka, s. 39.

positiva förslag och förstärka en annan dimension av processen, än att enbart försöka motverka andra initiativ. Det är nog särskilt viktigt på informationssäkerhetsområdet, där besluten fattas genom kvalificerad majoritet och där det inte finns någon möjlighet för en medlemsstat att blockera ett initiativ. Om man motsätter sig ett förslag utan att föreslå nya initiativ måste man ha tunga argument. Ett sådant kan t.ex. vara en hänvisning till att förslaget fullständigt går emot den nationella opinionen i flera medlemsstater.

Kontinuitet och enad front utåt

Kontinuitet och enad front utåt

Inom informationssäkerhetsområdet finns det troligen färre motsättningar staterna emellan än inom många andra områden. Det handlar till stor del om att driva en övergripande process framåt för att förbättra säkerheten. Ståndpunkterna inom ramen för denna skiljer sig inte åt på samma sätt som till exempel inom den europeiska säkerhets- och försvarspolitiken. Av den anledningen krävs det förmodligen inte kontinuitet i den bemärkelsen att svenska representanter i Bryssel har detaljkunskaper och vet exakt vad som ligger i linje med tidigare positioner och hållningen i angränsande frågor. Å andra sidan är det ett område som i stor utsträckning är spritt på många olika aktörer, såväl offentliga som privata, vilket gör att det är svårt att överblicka. Trots att frågorna inte är så kontroversiella och alltså inte ställer samma krav på nationell likriktning på detaljnivå, bör samordningen vara god för en enad front utåt. En sådan är en förutsättning för att ett land ska kunna åtnjuta förtroende inom EU. Om en liten stat som Sverige driver frågor i flera parallella spår, blir möjligheterna att nå inflytande mindre.

Nationell samordning och en enad front utåt kan uppnås på flera olika sätt. Man kan skapa en bas att utgå ifrån med hjälp av raminstruktioner till de olika nationella aktörer som representerar Sverige i Bryssel. Detta är viktigt eftersom det i sin tur skapar förutsättningar för att bygga upp argument, samtidigt som målen görs tydliga. Inte

minst beroende på personalomsättning och rotation är det viktigt att snabbt kunna skapa sig en överblick över frågorna och den drivna policyn.

”Näringslivet är en viktig aktör.”

Att utnyttja de nationella forum som finns i större utsträckning, alternativt skapa nya mötesformat för att diskutera EU-frågor som påverkar informationssäkerhet är ett annat sätt att skapa förutsättningar för en enhetlig ansats. Bland annat är det förmodligen bra metoder för att utöka informationsutbytet mellan den offentliga sektorn och näringslivet. Näringslivet är en viktig aktör inte bara på nationell nivå utan är även i stor utsträckning inblandat i olika expert- och referensgrupper på EU-nivå. Detta understryker behovet av ökat informationsutbyte mellan privat och offentlig sektor. Möten som hålls när en viss fråga blir aktuell på EU-nivå skapar emellertid inte den kontinuitet som krävs. Därför är det förmodligen bättre med ett stående mötesformat i sammanhanget.

Saabs Capability Development Centre på Saab i Järfälla. De har utvecklat ett system som gör att man kan samköra civila och miltära positionssystem. Det är speciellt intressant vid katastrofscenarion. Det är den första platsen i Sverige som skulle kunna fungera som en test- och träningsanläggning för att hantera en nationell kris, likt Tsunamin, stormen Gudrun eller ett möjligt och storskaligt terroristattentat. Foto: Henrik Montgomery.

Flexibilitet

Flexibilitet

Inom ett område som är så utspritt som informationssäkerhet är inom EU finns det inte resurser för en liten stat att driva en linje inom varje enskild fråga. Vissa förutsättningar måste därför vara uppfyllda för att en liten stat ska kunna bli framgångsrik på den gemensamma politiska arenan. Vi har tidigare framhållit vikten av prioriteringar. Dessa är starkt sammankopplade med förmågan att vara flexibel. Flexibilitet kan t.ex. yttra sig i riktlinjer snarare än snäva instruktioner. Riktlinjer ställer visserligen högre krav på personlig förmåga men gör också att man i större utsträckning kan välja sina strider. Då kan man driva de frågor som verkligen speglar ett viktigt intresse och där utsikterna att nå framgång också är störst. Eftergifter kan också förmedla en positiv bild av att man är en bra samarbetspartner som kan kompromissa när det krävs. Det visar dessutom på klart fokus och tydliga intressen.

Att mindre stater har mindre administrationer och ofta kortare beslutsvägar gör det möjligt för dem att vara mer flexibla vid snäva tidsramar och krav på att snabbt uppnå samsyn. En mindre stat har förmodligen också färre områden med starka nationella intressen, vilket gör den mer flexibel och ger den möjlighet att prioritera. Dessa fördelar måste utnyttjas för att Sverige ska kunna bli en framgångsrik aktör.

Slutligen är det även viktigt med en flexibel hållning till hur en fråga ska föras upp på EU-nivå för att kunna få gehör för sin politik. Informationssäkerhetsaspekter fogas ganska ofta in i initiativ som har ett annat huvudsyfte än att bidra till ökad informationssäkerhet. Om ett initiativ med tyngdpunkt på informationssäkerhet har väckts men inte fått gehör, kan det därför vara värt att undersöka möjligheterna att lyfta frågan inom ramen för ett initiativ som har ett annat syfte. Det kan t.ex. handla om ökad konkurrens eller tillväxt.

3 EU:s informations-säkerhetspolitik

Efter en kort, allmän introduktion till EU ger vi i det här kapitlet en bakgrund till EU:s informationssäkerhetspolitik och en beskrivning av några av de viktigaste aktörerna inom EU samt deras ansvarsområden. En mer heltäckande kartläggning av EU:s informationssäkerhetsarbete finns i rapporten "Vem gör vad inom EU? – informationssäkerhetsfrågorna i fokus".

3.1 Introduktion till EU[10]

Samarbetet inom EU kan delas in i 25 olika politikområden. Beroende på vilken av EU:s tre pelare ett politikområde hör till, kommer beslutsformerna att variera. Pelarindelningen markerar även vilken grad av inflytande medlemsstaterna har inom varje politikområde. Den första pelaren, EG, omfattar de flesta regler som rör EU:s inre marknad, som handelspolitiken och jordbrukspolitiken. Medlemsstaterna har i stor utsträckning överfört beslutsfattandet till EU inom denna pelare och det vilar med andra ord i regel på överstatlig grund. Inom den andra pelaren, den gemensamma utrikes- och säkerhetspolitiken (GUSP), är beslutsfattandet mellanstatligt till skillnad från i den första pelaren. Det innebär att en medlemsstat inte kan bli bunden av beslut som den motsätter sig. Även i den tredje pelaren, rättsliga frågor och inrikesfrågor (RIF), vilar samarbetet i huvudsak på mellanstatlig grund.

Första pelaren:
EU:s inre marknad

Andra pelaren:
Utrikes- och säkerhetspolitiken (GUSP)

Tredje pelaren:
Rättsliga frågor och inrikesfrågor (RIF)

EU:s organisation, maktbefogenheter och beslutsfattande regleras för närvarande av EG- och EU-fördragen. Vid Europeiska rådets möte i juni 2007 kom medlemsstaternas stats- och regeringschefer dock överens om innehållet i ett nytt så kallat reformfördrag. Därefter har en regeringskonferens med målsättningen att slutföra arbetet under

[10] Se t ex EU-upplysningens hemsida : www.eu-upplysningen.se eller EU-portalen: http://eur-lex.europa.eu/sv/droit_communautaire/droit_communautaire.htm.

EU-parlamentet i Strasbourg, Frankrike.
Foto: Bosse Nilsson.

hösten inletts. Förutsatt att det blir så, skulle det nya fördraget kunna träda i kraft under 2009.

Men det räcker inte med enbart fördragsbestämmelser för att reglera verksamheten inom EU:s olika politikområden. Det beror på att bestämmelserna i fördraget i stor utsträckning är t utformade. Inom varje pelare finns därför olika typer av bindande och icke-bindande rättsinstrument som fyller ut fördragsbestämmelserna med ett mer konkret innehåll.

Inom den första pelaren finns tre former av bindande lagstiftning: direktiv, förordningar och beslut. Direktiv är en form av ramlagstiftning vars syfte är att harmonisera medlemsstaternas lagstiftning. Varje direktiv har ett tydligt mål som är bindande för medlemsstaterna, men hur detta ska uppnås får varje medlemsstat bestämma självständigt. Förordningar å andra sidan är direkt tillämpliga i medlemsstaterna och är i alla delar bindande för samtliga som berörs av innehållet. Det tredje bindande rättsinstrumentet i den första pelaren är beslut. De riktar sig till medlemsstaterna, företag eller enskilda unionsmedborgare. Genom beslut kan EU:s institutioner bevilja stöd till eller ställa krav på en medlemsstat. Vidare kan institutionerna fatta beslut om rättigheter och skyldigheter för en enskild unionsmedborgare. Besluten är bindande för dem som de är riktade till.

I den andra pelaren finns det ingen bindande lagstiftning. Där fattas i stället beslut om olika former av rättsinstrument för att samordna medlemsstaternas agerande. Dessa kan delas in i gemensamma ståndpunkter, gemensamma åtgärder och beslut.

Den tredje pelaren innefattar bindande rättsinstrument, i likhet med den första. Det finns emellertid ingen motsvarighet till de direkt tillämpliga lagstiftningsformerna i den första pelaren. De så kallade rambesluten i den tredje pelaren liknar i stället direktiv i den meningen att de sätter upp mål för vad som ska uppnås och överlåter åt medlemsstaterna att besluta om genomförandet. Beslut i

tredje pelaren används för att uppnå samtliga mål som inte kräver harmonisering av medlemsstaternas lagstiftning.

3.2 Introduktion till EU:s informationssäkerhetspolitik[11]

EU:s arbete inom IKT och informationssäkerhetsområdet behandlas inte som ett separat politikområde inom EU-fördraget. I stället hanteras frågorna som en del av politikområdena om den inre marknaden, transportpolitik samt forskning och utveckling. EU:s informationssäkerhetsarbete kan härledas tillbaka till åtminstone mitten av 1980-talet. I början var syftet att stärka den ekonomiska tillväxten i EU genom att stödja den inre marknaden och EU:s konkurrenskraft gentemot den övriga världen. Informationssäkerhet blev viktigt inom EU:s arbete för att skapa ett informationssamhälle för alla. Informationssäkerheten sågs nämligen som nödvändigt för att man skulle kunna uppnå en tillräcklig nivå av säkerhet och tillförlitlighet hos det så kallade e-samhällets tjänster. Informationssäkerhetsarbetet har på senare tid utvecklats till att även innefatta frågor med tydligare säkerhetsfokus som berör medlemsstaternas nationella säkerhet och säkerheten för kritisk infrastruktur. Så har det blivit i takt med att europeisk utrikes- och säkerhetspolitik har utvecklats, och hotet från terrorister har blivit mer påtagligt.

3.3 Aktörer och ansvarsområden

Av EU:s olika institutioner är kommissionen av störst intresse. Den har ensam initiativrätt i den första pelaren och dessutom ett stort ansvar för den verksamhet som blir resultatet av EU:s beslut. Kommissionen har mer än tjugo generaldirektorat men som vi tidigare har nämnt finns det inget generaldirektorat som bär det samlade ansvaret för eller enbart hanterar informationssäkerhetsfrågor. I verkligheten finns det dock vissa aktörer som är mer inblandade än andra. De mest framträdande generaldirektoraten inom informationssäkerhetsområdet är generaldirektoratet för informationssamhället och medier

[11] Fylkner, M., Barck-Holst, S., Englund L., och Jarlsvik, H. (2006), "Vem gör vad inom EU? – informationssäkerhetsfrågorna i fokus".

(GD INFSO) och generaldirektoratet för rättvisa, frihet och säkerhet (GD JLS). Det finns också andra inblandade generaldirektorat, t.ex. generaldirektoratet för informationsteknik (GD DIGIT), generaldirektoratet för näringsliv (GD ENTR), generaldirektoratet för energi och transport (GD TREN) och det gemensamma forskningscentret (JRC). Den mest renodlade informationssäkerhetsaktören inom EU-strukturen är annars den europeiska nätverks- och informationssäkerhetsbyrån ENISA. Nedan beskrivs GD INFSO, GD JLS, GD DIGIT och ENISA mer i detalj.

3.3.1 Generaldirektoratet för informationssamhället och medier (GD INFSO)

Kommissionens generaldirektorat för informationssamhället och medier ska främja innovations- och konkurrenskraften i Europa. Det spelar därmed en betydande roll för Lissabonstrategin och i synnerhet i2010-initativet (se även kapitel 5). GD INFSO stödjer bland annat åtgärder för att stärka EU-regionens forskning och utveckling inom IKT-området.

Informationssäkerhet i fokus

Inriktningen på den verksamhet som generaldirektoratet för informationssamhället och medier ansvarar för innebär att det är en av de viktigaste aktörerna inom informationssäkerhetsområdet. Generaldirektoratet hanterar ett brett spektrum av sakfrågor, från en övergripande policynivå till forskningsfrågor. För att kunna hantera frågor med ett tekniskt djup och komplexitet har generaldirektoratet en ganska stor andel forskarutbildad personal. GD INFSO är ett av de generaldirektorat som har störst andel funktionärer med forskarbakgrund eller arbetslivserfarenhet från näringslivet.

Policyarbetet går till stor del ut på att se över nuvarande policyer för att de ska stämma med de riktlinjer som finns i Lissabonstrategin och i2010-initativet. Som exempel på relevanta initiativ kan vi lyfta fram det normerande arbetet inom elektronisk kommunikation (ELKOM) och dataskyddslagen.[12]

[12] Direktiv 2002/58/EG, om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

GD INFSO har flera initiativ och program som är relevanta för informationssäkerhetsområdet, från forskning till projekt som utmynnar i en senare marknadsintroduktion. Det största och kanske viktigaste området är forskningen inom IKT. IKT är dessutom det resursmässigt största området inom det sjunde ramforskningsprogrammet. Förutom den nämnda IKT-verksamheten ansvarar generaldirektoratet för olika program som stödprogrammet för informations- och kommunikationstekniker (ICT PSP) med syftet att uppfylla i2010:s mål. De olika initiativen samordnas internt inom generaldirektoratet men även med andra generaldirektorat för att undvika att samma arbete utförs på olika ställen. I stället vill man skapa en balans mellan forsknings-, utvecklings- och tillämpningssatsningar. Som ett led i att skapa ett gemensamt europeiskt informationsområde arbetar generaldirektoratet med information riktad mot både företag och privatpersoner

3.3.2 Generaldirektoratet för rättvisa, frihet och säkerhet (GD JLS)

Kommissionens generaldirektorat för rättvisa, frihet och säkerhet ska verka för att dessa värden upprätthålls inom EU:s gränser. Till skillnad från andra politikområden, t.ex. de som berör den inre marknaden, delar kommissionen och medlemsstaterna initiativrätten inom området

Informationssäkerhet i fokus

Generaldirektoratet för rättvisa, frihet och säkerhet har en viktig roll och ett stort ansvar när det gäller informationssäkerhetsfrågor med anknytning till polisiärt och straffrättsligt arbete. Arbetet innefattar frågor om cyberkriminalitet, men även frågor som berör den personliga integriteten. I arbetet för att skydda den personliga integriteten ingår åtgärder för att förhindra spridningen av barnpornografi på internet. Vidare var generaldirektoratet med och tog fram direktiv 95/46/EG om skydd av personuppgifter. Direktivet har legat till grund för den svenska personuppgiftslagen (PUL).

Offrens namn efter attacken den 11 mars på Atocha järnvägsstation. Foto: HADJ/SIPA.

Efter attentaten mot kollektivtrafiken i Madrid har skydd av kritisk infrastruktur (CIP) blivit en viktig fråga för EU. GD JLS har det övergripande ansvaret för CIP och skydd av kritisk informationsinfrastruktur (CIIP). Generaldirektoratet genomför både normerande processer som det sektorövergripande europeiska programmet för skydd av kritisk infrastruktur (EPCIP) och finansiering av studier och projekt inom programmet Prevention of and fight against crime.

3.3.3 Generaldirektoratet för informationsteknik (GD DIGIT)

Verksamheten vid kommissionens generaldirektorat för informationsteknik har framför allt förvaltande karaktär. Syftet med verksamheten är att stödja kommissionen genom att utveckla och förvalta en kommissionsomfattande infrastruktur för IKT. Infrastrukturen ska uppfylla kraven när det gäller säkerhet och tillförlitlighet och därmed skapa förutsättningar för att EU:s e-förvaltningsstrategier ska kunna genomföras.[13]

Generaldirektoratet ska samordna utvecklingen av teknik för informationssystem för samtliga avdelningar inom kommissionen. Det tillhandahåller dessutom IKT-tjänster för EU:s organ. Generaldirektoratet ansvarar även för att ta fram och verkställa en övergripande it-strategi som är i linje med kommissionens prioriteringar och behov.

[13] e-kommissionen 2006-2010; http://ec.europa.eu/dgs/informatics/ecomm/doc/ecomm-2006-2010_cs_en_v414_postcis.pdf.

Informationssäkerhet i fokus

GD DIGIT ansvarar för att den interna infrastrukturen inom kommissionen är säker och tillförlitlig. Därutöver driver generaldirektoratet e-förvaltningsprogrammet IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens), vars syfte är att utveckla e-förvaltningen i medlemsstaterna och förenkla samarbetet inom EU. Generaldirektoratet tog år 2007 över IDABC från generaldirektoratet för näringsliv och industri.

3.3.4 ENISA – Europeiska nätverks- och informationssäkerhetsbyrån

Den 10 mars 2004 antogs en förordning om inrättandet av EU:s nätverks- och informationssäkerhetsbyrå (ENISA). Byrån inrättades med huvudmålet att "säkerställa en hög nivå på nät- och informationssäkerhet i gemenskapen och utveckla en kultur av nät- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga sektorns organisationer i Europeiska unionen och på det sättet bidra till att den inre marknaden fungerar väl".[14]

Byrån ska bedriva sin verksamhet från och med den 14 mars 2004 till och med den 31 december 2008, då byråns förordnande går ut. ENISA genomgår just nu en utvärdering för att bedöma dess fortsatta status och inriktning. Meddelandet om utvärderingen av ENISA fastslås att byrån har fört en mer undanskymd tillvara än förväntat samtidigt som resultaten varit blygsammare. Utredningen påtalade även en bristande fokusering på verksamhetens effekter snarare än på produktion av material.[15]

Det finns en mängd orsaker som kan förklara den begränsade framgången. Utvärderingen poängterar till att börja med att medlemsstaterna inte har en samstämmig vision

[14] Förordning 460/2004/EG, om inrättandet av den europeiska byrån för nät- och informationssäkerhet.

[15] KOM/2007/285, utvärderingen av den europeiska byrån för nät- och informationssäkerhet (ENISA), s. 7.

om byrån och att det är oklart hur ENISA-förordningen ska tolkas, vilket t.ex. är synligt i relationen mellan byråns personal och styrelsen.[16] Byråns verksamhet begränsas dessutom av att den inte får inkräkta på eller förekomma, hindra eller dubblera de relevanta befogenheter och arbetsuppgifter som ligger på de berörda nationella regleringsmyndigheterna, de europeiska standardiseringsorganen och medlemsstaternas tillsynsmyndigheter.[17] En av ENISA:s viktigaste uppgifter är att utveckla samverkan med olika aktörer. Det är en uppgift som försvåras av det faktum att byrån ligger geografiskt svårtillgängligt, i Heraklion på Kreta. Den geografiska placeringen ska även ha bidragit till att försvåra rekryteringen och bidragit till en alltför hög personalomsättning.

Den externa utvärderingsgruppen påpekade att det fanns stora möjligheter för en europeisk byrå för nät- och informationssäkerhet, särskilt med tanke på att betydelsen av säkerhet fått ökad betydelse i EU. Utvärderingsgruppen menade även att ENISA skapar unika förutsättningar för att uppfylla behovet av samordning av säkerhetsfrågor inom EU och även som en motpart till globala allianser.

Både den externa utvärderingsgruppen och styrelsen för ENISA rekommenderar att förordningen bör förändras så att byråns mandat förlängs efter 2008. Ett offentligt samråd och en konsekvensbedömning kommer nu att komplettera rekommendationerna. Kommissionen kommer att informera Europaparlamentet och rådet om resultatet samt rapportera om de viktigaste slutsatserna, som eventuellt kommer att innehålla ett förslag om förlängning av byråns mandat.

Informationssäkerhet i fokus

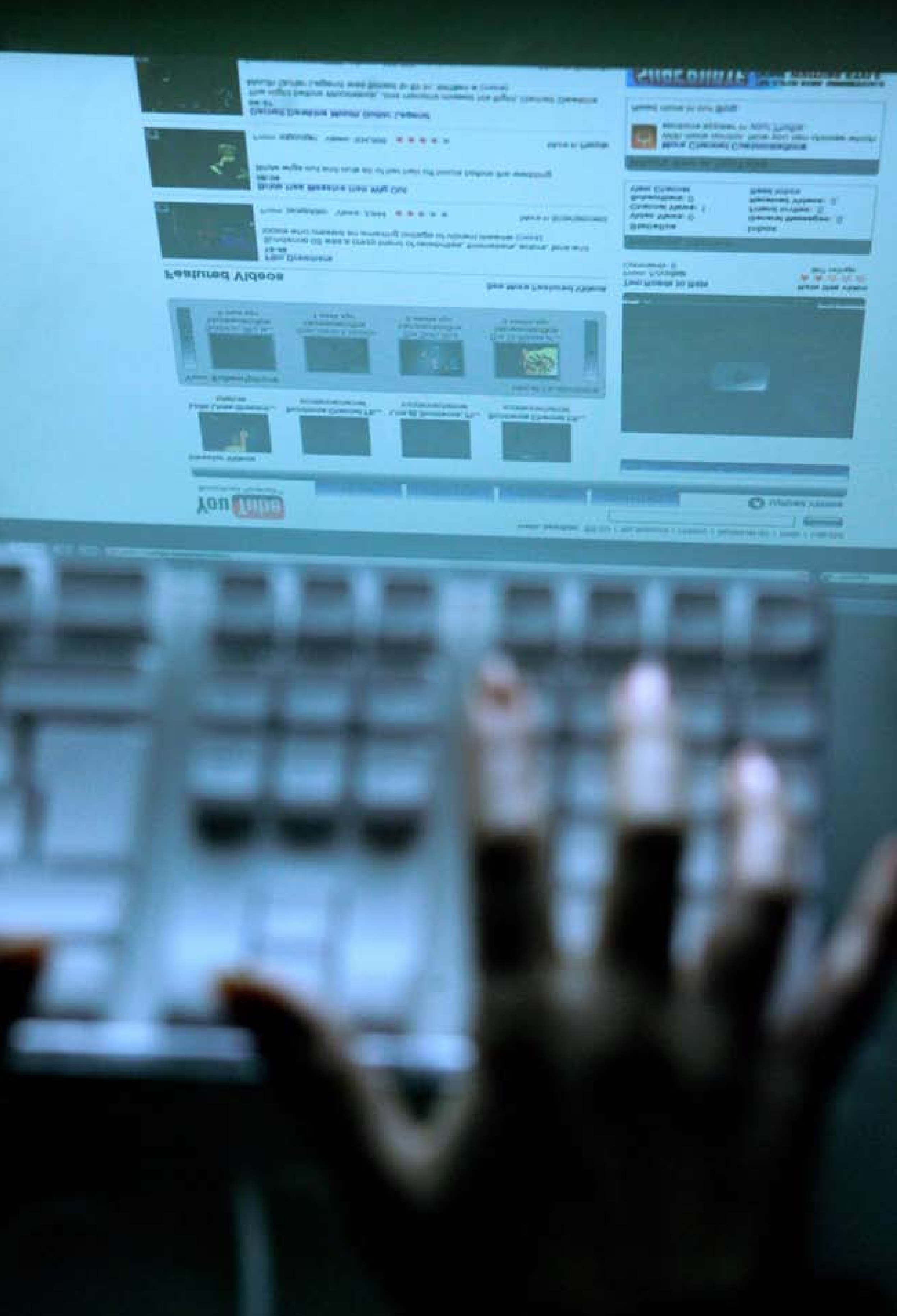
ENISA bedriver verksamhet på fem huvudsakliga teman: medvetandehöjande och förtroendeskapande åtgärder, främjandeverksamhet på den interna marknaden för elektronisk kommunikation, framväxande tekniker och tjänster, minskning av säkerhetsglappet i Europa samt samverkan och kommunikation.

[16] KOM(2007)285 s. 9.
[17] Förordning 460/2004/EG s. 2.

Byrån strävar efter att bli ett samverkansforum för informationsutbyte mellan alla relevanta aktörer och verkar för ett ökat samarbete inom nätverk- och informationssäkerhet. ENISA håller regelbundet samråd med aktörer från näringslivet, universiteten, representanter för medlemsstaterna och EU, anordnar seminarier och utvecklar ett kontaktnätverk. Byrån har också fått i uppdrag att bistå kommissionen och medlemsstaterna i den dialog med näringslivet som berör säkerheten hos datautrustning och mjukvara. Utöver att uppmuntra samarbeten i EU bidrar ENISA vid behov med råd och stöd till parlamentet och kommissionen samt hjälper unionen med att upprätta samarbeten med tredjeländer och med internationella organisationer.

En stor del av verksamheten består av analyser och medvetandehöjande åtgärder. Analyserna består ofta av kartläggningar av den befintliga statusen i EU-regionen inom ett område. Exempelvis har ENISA tagit fram en övergripande förteckning över vilka kontaktpersoner som finns i EU och medlemsstaterna inom nätverk- och informationssäkerhet. Byrån har också gjort en liknande kartläggning av befintliga CERT-grupper (Computer Emergency Response Team) i Europa. Sedan tillkommer risk- och hotbildsanalyser som kan ligga till grund för analyser av nuvarande och kommande risker, framför allt sådana som kan påverka de elektroniska kommunikationsnätens robusthet och den elektroniska kommunikationens autenticitet, tillförlitlighet och konfidentialitet. ENISA har även inventerat metoder och verktyg för riskhantering. När det gäller medvetandehöjande åtgärder har ENISA organiserat seminarier och utvecklat ett program för informationssäkerhetsmedvetande. ENISA har även framställt en användarmanual för hur man ökar informationssäkerhetsmedvetande".[18] I samma anda har byrån utvecklat en användarmanual för att uppföra en CERT.

[18] EDA publikationer; http://www.enisa.europa.eu/pages/05_01.htm.



4 Svenska statsmaktens viljeyttringar inom informationssäkerhets-området

I detta kapitel ger vi först en allmän introduktion till svenskt strategiarbete inom informationssäkerhetsområdet. Sedan följer en analys som identifierar ett antal svenska viljeyttringar som kan anses vara så pass viktiga att de kan bli en grund för en svensk strategi för att utöva inflytande på EU:s informationssäkerhetsarena. Eftersom FOI inte har mandat att fastställa svenska statsmaktens viljeyttringar och studien dessutom endast ska resultera i ett förstadium till en svensk strategi, finns det möjligheter att i ett senare skede se över valen av viljeyttringar

4.1 Introduktion till svenskt strategiarbete inom informationssäkerhetsområdet

Sveriges övergripande målsättning för informationssäkerhetsarbetet bör enligt proposition 2001/02:158 vara "att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet". För att vidareutveckla det svenska informationssäkerhetsarbetet tillsattes en informationssäkerhetsutredning vars uppgift var att lämna förslag på hur den nationella strategin bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom området bör utformas i framtiden.

"att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet"

Dataskärm. Foto: Sebastian Widmann.

Informationssäkerhetsutredningen utmynnade bland annat i ett förslag till en strategi där nedanstående tio punkter.[19]

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

I strategin bör även ingå att:

7. **Utnyttja samhällets samlade kapacitet.**
8. **Fokusera på samhällsviktig verksamhet.**
9. **Öka medvetenheten om säkerhetsrisker och möjligheter till skydd.**
10. **Säkerställa kompetensförsörjningen.**

"En utvecklad strategi bör ha ett långsiktigt perspektiv och utvecklas kontinuerligt."

Inriktningen på det svenska strategiarbetet är dock fortfarande otydligt i fråga om ämnesområden och tydliga prioriteringar. Regeringen valde i den efterföljande propositionen (2005/06:133) att endast betona att "en utvecklad strategi bör ha ett långsiktigt perspektiv och utvecklas kontinuerligt för att ligga till grund för handlingsplaner, prioriteringar och åtgärder på två till tre års sikt". I regleringsbrevet för år 2007 gav regeringen KBM i uppgift att

[19] SOU 2005:42 s. 10.

utveckla ett förslag till en handlingsplan för att genomföra och förvalta den nationella strategin för informationssäkerhet. Uppdraget kommer att slutredovisas i slutet av 2008

4.2 Kartläggning av svenska viljeyttringar

Eftersom Sverige saknar en strategi med tydligt utvecklade ämnesområden för informationssäkerhet genomfördes en analys av propositionerna (2001/02:158, 2005/06:133), informationssäkerhetsutredningen (SOU 2005:42 och SOU 2005:71) samt KBM:s lägesrapport 2007[20]. Syftet var att identifiera viljeyttringar, som i detta arbete representerar en utgångspunkt för vad som kan bedömas vara viktiga områden för Sverige när det gälle informationssäkerhet.[21] Med viljeyttring menar vi ett sakområde alternativt en process som har beskrivits vid flertalet tillfällen i informationssäkerhetsutredningen, propositionerna eller KBM:s lägesrapport 2007 och som vi därför bedömer som viktigt.

Resultatet från kartläggningen av svenska viljeyttringar ger inte svaret på vilka strategiska prioriteringar Sverige ska göra på nationell eller internationell nivå. Det ligger utanför FOI:s mandat. Med resultatet kan man däremot effektivare identifiera och precisera relevanta EU-processer och aktörer som hanterar viktiga frågeställningar ur ett svenskt perspektiv.

Nedan följer en beskrivning av identifierade viljeyttringar i fråga om tekniska medel, normering, ökad robusthet, samverkan, hantering av incidenter och kompetens.

4.2.1 Tekniska medel

I viljeyttringen tekniska medel ingår utveckling av IKT-verktyg med relevans för säkrare kommunikation och skydd av information. Verktygens art kan variera från lösningar för säkra transaktioner, autentiseringslösningar, utveckling av säkra nät och tillämpning av signalskydd.

[20] KBM:s lägesrapport 2007 – samhällets informationssäkerhet.

[21] Referenser för spårbarhet återfinns i bilaga 1 – Kartläggning av svenska viljeyttringar.

Viljeyttringen tekniska medel innefattar samtliga faser från att en produkt befinner sig i ett tidigt utvecklingsskede till att en den är färdig för lansering på marknaden.

4.2.2 Normering

Informationssäkerhetsutredningen påpekar att det är staten som bör ansvara för spelreglerna inom informationssäkerhetsområdet.[22] Utredningen betonar även vikten av att det författningsmässiga stödet utvecklas samt att en den internationella lagstiftningen bör samordnas mer. De här åtgärderna skulle kunna stärka verksamheten inom informationssäkerhetsområdet. Med viljeyttringen normering menar vi att man normerar och underlättar verksamheten inom området med hjälp av olika regleringsverktyg. Detta sker främst genom traditionella regleringsverktyg som lagstiftning och förordningar, men även genom utveckling av exempelvis standarder.

4.2.3 Ökad robusthet

Bredbandsanslutning. Foto: Göran Billeson.

Den kritiska infrastrukturen inom bland annat el, tele, betalningssystem och vattenförsörjning är så vital för att samhället ska kunna fungera att det inte är acceptabelt att den slås ut av en IKT-relaterad incident.[23] Med robusthet menar vi här ett systems förmåga att stå emot yttre och inre påfrestningar. Med viljeyttringen ökad robusthet menar vi att man minskar sårbarheten i befintliga system och verksamheter genom olika åtgärder. I viljeyttringen ingår också att man ökar den specifika nodens (systemets) motståndskraft för IKT-attacker.

4.2.4 Samverkan

Informationssäkerhetsutredningen föreslår att utgångspunkten för informationssäkerhetsarbetet bör vara att bättre utnyttja samhällets samlade kapacitet på området. Samverkan mellan olika aktörer skapar större förutsättningar för att tillgodogöra sig utvecklingen inom olika områden, sektorer och geografiska platser. Informations-

[22] SOU 2005:42 s. 85.
[23] Ibid s. 87.

säkerhetsutredningen rekommenderar ett ökad internationellt samarbete, ökad samverkan inom offentlig sektor samt ökad samverkan mellan offentlig och privat sektor. Utredningen nämner speciellt förbättrad spridning av underrättelseinformation. Viljeyttringen samverkan innefattar alla former av samverkan som är relevanta för informationssäkerhetsområdet.

4.2.5 Hantera incidenter

Viljeyttringen hantera incidenter omfattar den förmåga att hämta och bearbeta information som man måste ha för att kunna agera i alla faserna av en incidenthanteringscykel. Om man har den förmågan kan man skapa ett organisatoriskt system för informationssäkerhetsarbetet som garanterar kontinuitet och kvalitet. I incidenthanteringscykeln ingår att förebygga, upptäcka, identifiera, ingripa och återställa verksamheten.

4.2.6 Kompetens

Enligt informationssäkerhetsutredningen är det av strategisk betydelse att se till att det finns tillräckligt mycket kompetent personal inom informationssäkerhetsområdet. Det gäller både den grundläggande utbildningsnivån och kvalificerad forskning. Enligt informationssäkerhetsutredningen är medvetandet om sårbarheter, hot och risker hos enskilda användare och kunskapen om vilka skyddsåtgärder som finns på marknaden på en sådan nivå att särskilda insatser är motiverade. Viljeyttringen kompetens omfattar ett brett spektrum av åtgärder för att öka förståelsen för informationssäkerhet i samhället. Det handlar om allt från folkbildning till ren forskningsverksamhet.

5 Att påverka EU:s informationssäkerhetspolitik

I det här kapitlet placerar vi EU:s informationssäkerhetspolitik i ett svenskt sammanhang genom att lägga de svenska viljeyttringar som identifierades tidigare i studien som ett raster på EU:s informationssäkerhetsarbete. Kapitlet inleds med en beskrivning av EU:s strategiska ramverk för IKT-området – i2010 (exempel på en viktig fråga i kategorin "vad?") och en analys av svenska påverkansmöjligheter i form av när och hur Sverige bör agera. Därefter ger vi exempel på varje enskild svensk viljeyttring (exempel på viktiga frågor i kategorin "vad?") med de initiativ inom EU:s informationssäkerhetsarbete som är relevanta för de svenska viljeyttringarna. För varje viljeyttring analyserar vi svenska påverkansmöjligheter utifrån när och hur Sverige bör agera inom det aktuella området. Som utgångspunkt för analysen använder vi de generella byggstenar för strategiskt agerande som vi presenterade i början av rapporten.

5.1 i2010 – EU:s strategiska ramverk för IKT-området

EU:s informationssäkerhetsarbete utgår i stor utsträckning från i2010-initativet som är kommissionens strategiska ramverk för informationssamhället och en viktig del av det förnyade Lissabonpartnerskapet för tillväxt och sysselsättning.[24] i2010 skall säkerställa att kommissionens politik avseende informationssamhället och medier är enhetlig och bidra till att stärka den viktiga roll som IKT spelar för medlemsstaternas ekonomier.

i2010 ska säkerställa att kommissionens politik för informationssamhället och medier är enhetlig, och bidra till att stärka den viktiga roll som IKT spelar för medlemsstaternas ekonomier.

[24] KOM/2005/229, i2010 – Det europeiska informationssamhället för tillväxt och sysselsättning.

Svenska flaggan utanför Europeiska parlamentet, Bryssel. Foto: Stefan Borgius.

i2010 är en fortsättning på och utveckling av eEurope-initativen. År 1999 presenterade kommissionen initiativet eEurope 2002 i syfte att till fullo ta tillvara på möjligheterna som ett informationssamhälle kan ge.[25] Man ansåg att eEurope 2002 var ett framgångsrikt format för det strategiska arbetet för att utveckla ett europeiskt informationssamhälle och initiativet följdes av eEurope2005, vars handlingsplan godkändes av rådet under år 2002. Kommissionen började arbeta med att utforma i2010-initiatvet under 2004 och halvtidsutvärderingen av eEurope2005 var en viktig utgångspunkt för det arbetet. Kommissionen lyssnade på synpunkter från intressenter bland medlemsstaterna, näringslivet och universiteten och höll konferenser och konsultationer på webben. Under konsultationsprocessen la kommissionen mest kraft på att identifiera policyprioriteringar samt på att skapa kortsiktiga initiativ av kritisk art. Inom ramen för i2010-initiativet har kommissionen identifierat tre särskilt prioriterade huvudområden, nämligen[26]

- **att skapa ett gemensamt europeiskt informationsområde**
- **att främja en öppen och konkurrenskraftig inre marknad**
- **att stärka innovation och investeringar i forskning inom informationsteknologi.**

De tre huvudområdena har utvecklats från de ursprungliga syftena med eEurope. De är att få in samtliga aktörer in i den digitala eran och på webben, skapa ett digitalt kunnigt Europa samt att se till att processen är socialt inkluderande.

Inom i2010 bedrivs olika verksamheter för att främja utvecklingen inom IKT-området. Verksamheterna kan ta sig utryck i olika strukturer, men man kan belysa i2010:s sammanhållande betydelse med att samtliga program

[25] eEurope – An Information Society For All, Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000.
[26] KOM/2005/229 s. 4.

inom kommissionen som är relevanta för informationssäkerhetsområdet kan sammankopplas med i2010.


Röstning i EU-parlamentet, Strasbourg. Foto: Christian Lut.

Arbetet inom i2010 leds av generaldirektoratet för informationssamhället och medierna. Generaldirektoratet bevakar och samordnar IKT-verksamheten som sker i kommissionens regi och värderar den gentemot det pågående policy- och strategiarbetet. För att genomförandet av i2010 ska utvecklas enligt planerna och i enlighet med medlemsstaternas vilja har kommissionen skapat en s.k. high level group (i2010 HLG) med representanter från medlemsstaterna. Sverige representeras här av näringsdepartementet. Gruppen sammanträder tre gånger per år och tanken är att den ska vara ett forum för att lyfta fram relevanta IKT-frågeställningar. Gruppen är klassad som en expertgrupp och ska framför allt ge kommissionen råd om hur i2010-arbetet ska fortskrida och utvecklas. Den har även en utvärderande roll och ska utvärdera hur effektivt arbetet är, samt ge förslag till förbättringsmöjligheter och justeringar.[27] *E*U genomför årligen en i2010-konferens med seniora representanter från medlemsstaterna och industrin. Konferensen anordnas av det land som innehar ordförandeskapet i EU. På konferensen hanterar man övergripande policyfrågor som berör utvecklingen av informationssamhället.

Verksamheten inom IKT-området är till sin natur beroende av en säker infrastruktur för att målen ska kunna förverkligas. Informationssäkerhetsaspekterna är särskilt viktiga för ett gemensamt europeiskt informationsområde. Det avspeglar sig i att kommissionen har utvecklat ett åtgärdsprogram med initiativ oc*h åtgärder för att öka* nätverkssäkerheten.[28] Åtgärdsprogrammet omfattar en mängd olika initiativ och har utmynnat i meddelanden för en ny säkerhetsstrategi för informationssamhället, elektroniska signaturer, spam, och initiering av nya program som Safer Internet plus och European programme for critical infrastructure protection (EPCIP).

[27] Beslut 2006/215/EG, inrättande av en expertgrupp på hög nivå för rådgivning till Europeiska kommissionen om genomförande och utveckling av strategin i2010.
[28] KOM/2007/146, i2010 – Årsrapport om informationssamhället 2007.

Påverkansmöjligheter

Arbetet inom i2010 sker främst på en övergripande nivå. Man behandlar främst policyfrågor och inriktningen av IKT-verksamheten i stort och det är alltså sådant som kan påverkas inom ramen för initiativet, snarare en utveckling av specifika lösningar.

EU:s strategiska ramverk utvärderas och modifieras löpande. Det finns därmed ständigt förutsättningar att komma med synpunkter på hur det utformas. Störst möjlighet att påverka och förändra utformningen finns i samband med genomförandet av stora moment som halvtidsutvärderingen av i2010 och den eventuella processen för att initiera ett nytt initiativ när i2010 har avslutats. Halvtidsutvärderingen av i2010 ska vara slutförd 2008. Den kommer att fokusera på utmaningar på policynivå inom områdena framväxande trender inom nätverk och internet, användarperspektivet och den interna marknaden. Sverige skulle kunna lyfta informationssäkerhetsperspektivet inom dessa områden och därmed göra det lättare att driva informationssäkerhetsfrågor under EU-ordförandeskapet, hösten 2009. Under ordförandeskapet kommer även i2010 att gå mot sitt slut, och ett eventuellt efterkommande program börjar ta sin form.

Om man vill påverka inriktningen av policynära frågor är det viktigt att ta tillvara på de möjligheter som uppkommer. Med andra ord måste svenska representanter vara väl införstådda i den övergripande informationssäkerhetspolitik som Sverige vill driva. De bör också veta vilka personer som de kan kontakta för att snabbt få stöd i sak- och processfrågor. Därför krävs det att Sverige utvecklar formerna för samverkan mellan departement, myndigheter, näringsliv och universitet. Dessa aktörer är idag inblandade i olika delar av EU:s informationssäkerhetsarbete. Om Sverige tar fram en enad behovsbild med tydliga prioriteringar, får landet större möjligheter att påverka utvecklingen från olika håll och i olika forum. Samtidigt kan vi hålla en enad front och en konsekvent linje.

Ett forum för att påverka utvecklingen är expertgruppen i2010 HLG. Då gruppen består av höga ämbetsmän kan en fråga kan få genomslagskraft om den lyfts fram i detta forum. Under sitt ordförandeskap koordinerade Finland verksamheten med sin inhemska industri. Exempelvis presenterade Nokia sin syn på interoperabilitet och standardisering under det tredje i2010 HLG-mötet den tolfte december 2006.

I forum som behandlar policynära frågor i likhet med i2010:s s.k. high level group är det betydelsefullt att Sverige representeras på regeringskanslinivå eller möjligen av lämplig generaldirektör. Det är dock av central betydelse att Sveriges representant dessutom får stöd från experter inom sakområdet. Under det svenska ordförandeskapet vore EU:s årliga i2010-konferens ett lämpligt forum för att driva frågor som berör informationssäkerhet.

5.2 Svenska viljeyttringar inom ramen för EU:s informationssäkerhetspolitik

I följande avsnitt placerar vi EU:s informationssäkerhetsarbete i ett svenskt sammanhang, utifrån de sex viljeyttringar som vi identifierade tidigare. Viljeyttringarna är tekniska medel, normering, ökad robusthet, samverkan, hantering av incidenter och kompetens. EU:s verksamheter inom informationssäkerhetsområdet kommer oundvikligen att skära över en eller flera svenska viljeyttringar. De kommer därför att presenteras under den viljeyttring som mest berörs av ämnet och berörs endast kort under andra viljeyttringar.

5.2.1 Tekniska medel

Med tekniska medel menar vi verktyg och metoder för att utnyttja IKT. Inom informationssäkerhetsområdet kan verktygen variera från exempelvis signalskydd och säkra nät till autentiseringslösningar. Kommissionen bedriver

ingen konkret utvecklingsverksamhet i egen regi för att öka nät- och infrastruktursäkerheten i EU. Det enda undantaget är utvecklingen och förvaltningen av den egna interna infrastrukturen inom kommissionen. Däremot har unionen tillgång till finansiella verktyg och kan därigenom stödja utvecklingsprojekt av tekniska medel.

Programmen för tekniska medel avser att komplettera forskningssatsningarna inom bland annat det sjunde ramforskningsprogrammet genom att stödja projekt som befinner sig närmare en marknadsintroduktion. Intressenterna inom programmen för tekniska medel och forskningsprogrammen samverkar för att undvika att olika aktörer gör samma saker och att det blir obalans mellan forskning, utveckling och tillämpningssatsningarna.

EU:s stöd för utveckling av tekniska medel riktar sig idag framför allt mot initiativ för tillväxt inom IKT-området alternativt för att förbättra och effektivisera e-förvaltningen inom och mellan medlemsstaterna samt EU-institutionerna. Den senaste tiden har kommissionen även börjat stödja verksamhet med säkerhetsfokus och då framför allt beträffande kritisk infrastruktur. Nedan ger vi exempel på EU:s arbete med tekniska medel, genom en beskrivning av ett tillväxtorienterat IKT-stödprogram (ICT PSP) respektive ett e-förvaltningsprogram (IDABC).

Stödprogrammet för informations- och kommunikationsteknik (ICT PSP)

Det mest omfattande programmet för tekniska medel är stödprogrammet för informations- och kommunikationsteknik (ICT PSP) som är en del av ramprogrammet för konkurrenskraft och innovation (CIP).[29] Ramprogrammet för konkurrenskraft och innovation etablerades som en respons på halvtidsutvärderingen av Lissabonstrategin. Det primära syftet är att öka Europas konkurrenskraft och innovationskapacitet samt att bidra till en hållbar utveckling baserad på en balanserad ekonomisk tillväxt.[30] Ramprogrammet, som drivs av generaldirektoratet

[29] CIP – Competitiveness and Innovation framework Programme.
[30] Beslut 1639/2006/EG, upprätta ett ramprogram för konkurrenskraft och innovation (2007–2013).

för näringsliv och industri, håller nu på att genomföras. Programmets budget motsvarar 3,6 miljarder euro för perioden 2007–2013.

För att uppnå målet med ramprogrammet har kommissionen skapat tre särskilda program där ICT PSP är mest relevant ur ett informationssäkerhetsperspektiv. Åtgärderna inom IKT-stödprogrammet ska bidra till att uppfylla i2010:s strategiska mål: att skapa ett gemensamt europeiskt informationsområde med en öppen och konkurrenskraftig inre marknad samt ett starkt innovationsklimat inom informations- och kommunikationsteknologi. Stödprogrammet omfattar insatser som berör:

- utvecklingen av ett gemensamt europeiskt informationsområde och stärkande av den inre marknaden för IKT-produkter, IKT-tjänster samt IKT-baserade produkter och tjänster

- stimulans av innovation genom mer omfattande användning av och investering i IKT

- utveckling av ett informationssamhälle för alla samt mer ändamålsenliga och effektiva tjänster på områden av intresse för allmänheten, liksom förbättring av livskvaliteten.

Verksamheten inom stödprogrammet preciseras i årliga arbetsprogram där den totala budgeten motsvarar 728 miljoner euro, fördelat över programmets period 2007–2013. ICT PSP leds av generaldirektoratet för informationssamhället och medier, till skillnad från det övergripande CIP, som leds av generaldirektoratet för näringsliv och industri.

Stödprogrammet fokuserar främst på tillväxtorienterade åtgärder och har behandlat informationssäkerhetsfrågorna ur det perspektivet. I programmets första utvecklingsskede har informationssäkerhetsfrågorna funnits med som en garant för att de IKT-baserade tjänsterna ska kunna utnyttjas obehindrat och med bibehållet förtroende från

användarna.[31] Programmet betonar vikten av åtgärder som skyddar användarnas privatliv.

"Skapa säkra och lättanvända elektroniska identitets-lösningar"

Det är framför allt under genomförandefasen från och med att arbetsprogrammet tas fram som informationssäkerhetsfrågorna utvecklas och får ett större utrymme. Inom arbetsprogrammet har informationssäkerhetsfrågorna fått mest utrymme inom området eGovernment. Syftet med området är att förenkla och effektivisera den offentliga förvaltningens interaktion med andra aktörer. För att göra detta möjligt ska stödprogrammet bidra till ökad användning av elektroniska identiteter för offentliga tjänster. Det ska också skapa säkra och lättanvända elektroniska identitetslösningar som får en spridning inom EU.

När GD INFSO har tagit fram arbetsprogrammet, har de samarbetat med olika aktörer som exempelvis i2010:s s.k. high level group, i2010-arbetsgrupper och andra rådgivande intressentgrupper.

E-förvaltningsprogram (IDABC)

E-förvaltning är ett område där informationssäkerhet är viktigt. E-förvaltning har ett stort utrymme inom IKT-stödprogrammet, men utvecklingen av alleuropeiska elektroniska förvaltningstjänster för medborgare och företag sker framför allt inom programmet IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens). IDABC-programmet är sektorövergripande och används av generaldirektoraten och medlemsstaterna när de behöver starta utvecklingsprojekt för e-förvaltning.

IDABC-programmet är planerat för perioden 2005–2009. Programmet leds av generaldirektoratet för informationsteknik och har en sammanlagd budget på 148,7 miljoner euro. IDABC är en fortsättning på IDA (Interchange of Data between Administrations) och IDA II. IDA-programmet startade redan 1995 och har utvecklats till att bli allt mer affärs- och tjänsteorienterat.

[31] KOM/2005/121, upprättande av ett ramprogram för konkurrenskraft och innovation (2007-2013).

Målet med IDABC är att:

- möjliggöra informationsutbyte mellan offentliga förvaltningar i medlemsstaterna liksom mellan dessa förvaltningar och EU-institutionerna

- göra det lättare för företag och medborgare att få tillgång till alleuropeiska tjänster allt efter deras behov.

IDABC:s verksamhet omfattar både sektorspecifika och sektorövergripande (horisontella) aktiviteter. De sektorövergripande aktiviteterna tenderar att ha en större omfattning och budget. Dessa omfattar också övergripande åtgärder med syfte att skapa alleuropeiska e-förvaltningstjänster och infrastrukturtjänster, främst sådana som gagnar interoperabilitet. Åtgärderna kan exempelvis resultera i övergripande arkitekturarbete och riktlinjer för att möjliggöra interoperabilitet mellan förvaltningar i olika medlemsländer. Det kanske viktigaste projektet för Sverige är TESTA.

Genomförandefasen består främst av två delar, nämligen att fastställa vilka aktiviteter som ska genomföras inom ramen för arbetsprogrammet samt att fatta beslut om anslagsfördelning. Arbetsprogrammet uppdateras vid flera tillfällen under ramprogrammets gång.

Det är viktigt att beakta säkerhetsaspekten när man utvecklar och förvaltar IKT-system och tjänster. IDABC-programmet hanterar informationssäkerhet när det gäller utvecklingsfrågor men också frågor av mer strategisk art. Informationssäkerhetsfrågorna är typiska horisontella frågor. Inom programmen för informationssäkerhet arbetar man t.ex. med frågor om att knyta samman PKI-lösningar i olika länder (bryggning) och med att utfärda certifikat inom kommissionens förvaltningar. Därutöver genomför aktörerna studier om elektroniska signaturer och elektronisk identifiering för att förenkla administrationen.

Påverkansmöjligheter

Processen för de olika programmen för tekniska medel har många beröringspunkter med varandra. I de inledande initiativ- och beslutsfaserna hanteras mer övergripande frågor om initiativets innehåll. Det gör att informationssäkerhetsfrågor som ska betraktas som en integrerad del av processen får mindre utrymme. Det är dock viktigt att så tidigt som möjligt skapa förutsättningar för att påverka initiativets innehåll och inriktning.

Det är viktigt att vara uppmärksam på förändringar redan tidigt i processen. Svenska representanter bör därför se till att få en central roll i arbetsprocessen. Alternativt kan nationella experter placeras på strategiskt lämpliga positioner inom kommissionen. För att påverka inriktningen är det dessutom nödvändigt att de svenska representanterna i början av processen är insatta dels i hur den politiska processen utformas, dels i informationssäkerhetsfrågorna i sak. Det är därmed avgörande att tidigt i processen samordna sig nationellt och lyfta frågan nationellt genom samråd och seminarier, där representanter för samtliga berörda sektorer deltar.

Informationssäkerhetsaspekter tenderar att få ett större utrymme i en senare del av processen och då främst i genomförandefasen från och med att arbetsprogrammet fastställs. Därför är det viktigt att svenska aktörer är särskilt aktiva i denna fas. Sverige är en av de ledande nationerna inom informationssäkerhetsområdet när det gäller sakkunskap och har därmed mycket att bidra med på arbetsgruppsnivå. Sakkunskap räcker dock inte alltid. För att förstå helheten är det viktigt att känna till den politiska processen. För att representanterna ska kunna utnyttja denna fördel och påverka programmens utformning och inriktning, behöver de stöd från de som fattar beslut inom programmen. Inom vissa initiativ har det dock kommit fram att myndigheter och regeringskansliet inte samarbetar strukturerat. I stället är kontakterna informella, och det finns alltså inte någon plattform att utgå från för att driva en fråga framåt.

För att få så stort inflytande som möjligt är det viktigt att se till att de svenska representanterna kan tillräckligt mycket, dels om processen, dels om själva sakfrågan. Kan de inte det, är det viktigt att de får nödvändigt stöd via kända, upparbetade kanaler så att Sverige kan göra det som krävs för att nå framgång. För att förbättra förutsättningarna för de svenska experternas arbete bör de få gå introduktionskurser i EU:s beslutsprocess, och därmed få en större förståelse för helheten.

Generaldirektoraten söker i allt högre utsträckning stöd hos rådgivande grupper via inofficiella kanaler för att på så vis effektivisera processen. Att effektiviteten brister beror bland annat på att representanterna i arbetsgrupperna ofta är generalister snarare än informationssäkerhetsexperter. Ett annat problem är att representanterna ibland saknar det mandat från hemlandet som de behöver för att föra processen framåt. Deras uppgift har snarare varit att bevaka händelseutvecklingen och rapportera till sina överordnade. För att arbetet ska gå framåt har kommissionen byggt upp informella samarbeten som tidvis får stort inflytande. Nätverket kan bestå av olika former av intressegrupper eller konsortier (sammanslutningar) från näringslivet, enskilda forskare från universitet såväl som experter från medlemsstaterna. Dessa samarbetsgrupper utför mycket av det arbete som blir viktigt när det är dags att fatta formella beslut. Det förekommer t.ex. ganska ofta att kommissionen kontaktar personer som samordnar större EU-projekt för att ge synpunkter kring utformningen av kommande områden inom ramprogrammen eller arbetsprogrammen.

För att få inflytande över EU:s informationssäkerhetsarbete är det viktigt att bli en central aktör både inom de officiella och inom de inofficiella processerna. Som liten nation måste Sverige välja vilka frågor och processer man aktivt ska försöka utöva inflytande över. Därför är det nödvändigt att prioritera. Det är dessutom viktigt för en liten aktör att samordna resurserna för att få maximalt inflytande. EU och industrin har t.ex. ett gemensamt intresse av att industrin deltar aktivt i processen, eftersom syftet med

EU:s arbete inom utveckling av tekniska medel till stor del är att skapa förutsättningar för tillväxten inom unionen. Svensk industri (och svenska universitet) har mycket att tillföra i form av sakkunskap och har därmed stora möjligheter att bidra. Genom att utveckla samarbetsformer mellan industrin, universitet och myndigheter kan synergier uppnås. Den svenska samordningen och prioriteringen ska utgå från en gemensam svensk ståndpunkt.

Det är inte bara att samordna sig nationellt som är viktigt. Koalitioner mellan medlemsländer har blivit allt vanligare. Genom att gå samman med andra aktörer i ett tidigt skede av processen och gemensamt föra arbetet framåt, kan man öka sannolikheten för framgång.

5.2.2 Normering

Normering på EU-nivå sker i första hand genom olika typer av lagstiftning, men också genom mjukare former av styrning som t.ex. standardisering. I detta avsnitt åskådliggör vi EU:s normerande arbete som har betydelse för informationssäkerhet. Vi ger två exempel på lagstiftande åtgärder: det europeiska programmet för kritisk infrastruktur (EPCIP) samt översynen av EU:s regelverk för elektronisk kommunikation (ELKOM). Vi analyserar inte möjligheter att påverka inom området, eftersom EU:s roll inom standardisering kring informationssäkerhet är mycket begränsad.

Europeiska programmet för kritisk infrastruktur (EPCIP)

Frågan om risken för terroristattacker mot europeisk infrastruktur hamnade i fokus genom terrordåden i Madrid 2004. Det blev tydligt att angrepp mot kritisk infrastruktur kunde få konsekvenser för flera medlemsstater och på sikt påverka hela den europeiska ekonomin negativt. Diskussionen om en gemensam sektorsövergripande strategi för skydd av kritisk infrastruktur tog fart på allvar. Det blev början på den process inom CIP (Critical Infastructure Protection) och CIIP (Critical Information Infrastructure Protection) som i november 2006 utmynnade

i ett förslag till direktiv för att inrätta EPCIP,[32] ett av få initiativ med koppling till informationssäkerhet där tyngdpunkten ligger på säkerhet.

Eftersom förslaget uppstod i arbetet mot terrorismen, har GD JLS varit ansvarigt för arbeta fram förslaget. Inom GD JLS har en undergrupp för teknisk infrastruktur fört arbetet framåt. Den inrättades under den sektorsövergripande arbetsgruppen för interna aspekter på terrorism (Inter-Service Group on the Internal Aspects of Terrorism).

Här presenterar vi de viktigaste beståndsdelarna i det ramverk som ska utgöra grunden för EPCIP.

- Programmet ska ta fram ett förfarande för att fastställa och klassificera europeisk kritisk infrastruktur (ECI). Direktivet definierar vad som menas med europeisk kritisk infrastruktur. Vidare slår det fast att medlemsstaterna ska enas om detaljerade sektorsspecifika kriterier för att identifiera konkreta anläggningar. Dessa ska sedan rapporteras in till kommissionen och ligga till grund för en sammanställning av all ECI. Ägarna till anläggningarna ska upprätta säkerhetsplaner som omfattar de kritiska anläggningarna. I säkerhetsplanerna ska de ange vilka skyddsåtgärder som de har vidtagit. Medlemsstaternas myndigheter får till uppgift att utöva tillsyn över anläggningarna. Slutligen ska en kontaktpunkt utses för att samordna arbetet. I dagsläget finns denna kontaktpunkt vid KBM.

- Åtgärder för att underlätta genomförandet ska vidtas. En handlingsplan för EPCIP ska upprättas. Inom ramen för denna ska EPCIP regelbundet ses över. Vidare skapas ett nätverk för informationsutbyte (CIWIN – Critical Infrastructure Warning Information), expertgrupper på EU-nivå samt förfaranden för informationsutbyte.

[32] KOM/2006/0787, förslag till Rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna.

Under våren och sommaren 2007 har rådsarbetsgruppen för skydd och beredskap (PROCIV) behandlat förslaget till direktiv. Vid förhandlingarna har processen mött ett visst motstånd. De flesta medlemsländer är visserligen i grunden positiva till ett gemensamt ramverk för skydd av kritisk infrastruktur. Flera länder (däribland Sverige) anser dock att förslaget som det ser ut nu går längre än vad som är motiverat.

Kommissionen med GD JLS i spetsen föreslog dock att medlemsstaterna ska anta ny lagstiftning senast den 31 december 2007, i den mån det krävs för att direktivet ska implementeras. Frågan befinner sig nu i beslutsfasen, och om kommissionens tidsplan följs kommer genomförandefasen alltså i höst. Då får genomförandekommittén som tillsätts ta ställning till de sektorsspecifika kriterierna. Det är de generaldirektorat inom kommissionen som har ansvar för de kritiska sektorernas politikområden som har utvecklat dessa.

I takt med att informationsinfrastruktur har blivit allt viktigare för att upprätthålla olika samhällsfunktioner har många länder vidtagit åtgärder för att skapa ett skydd för kritisk informationsinfrastruktur. Eftersom informationsinfrastrukturen är gränsöverskridande, är det dock inte så effektivt med bara nationellt utformade skydd. Det är därför väsentligt att frågan tas upp på den gemensamma politiska arenan, via EPCIP.. I bilagan till den grönbok om kritisk infrastruktur som kommissionen presenterade under 2005 definieras CIIP som:

"the programs and activities of infrastructure owners, operators, manufacturers, users and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage."[33]

[33] KOM/2005/576, grönbok om ett europeiskt program för skydd av kritisk infrastruktur.

CIIP är inte begränsat till någon särskild sektor utan ska betraktas som en integrerad del av CIP. Det krävs med andra ord ett helhetsperspektiv på processen, där informationssäkerhetsaspekter är väl samordnade med problematiken inom de sektorer som har identifierats som kritiska.

Hur utvecklingen kommer att se ut inom CIIP-området beror på utvecklingen inom de olika kritiska sektorerna. Så länge som de sektorsspecifika kriterierna för vad som ska betraktas som kritisk infrastruktur inte har offentliggjorts, går det därför knappast att mer detaljerat beskriva vilka åtgärder programmet omfattar när det gäller kritisk informationsinfrastruktur.

CIWIN, nätverket för varningar om hot mot kritisk infrastruktur, har dock kopplingar till informationssäkerhetsområdet. Som vi tidigare har nämnt, är CIWIN en del av det gemensamma ramverk som EPCIP föreslås bestå av. Syftet med nätverket är att underlätta informationsutbyte i fråga om gemensamma hotbilder och sårbarheter inom EU. Tanken är att det ska komplettera befintliga nätverk.

En annan central aspekt ur informationssäkerhetssynpunkt, men även ur ett bredare perspektiv, är samverkan mellan privat och offentlig sektor. Eftersom de flesta operatörer och ägare av kritisk informationsinfrastruktur är privata, krävs det att samtliga aktörer medverkar i utvecklingen och vidareutvecklingen av programmet för att man ska kunna uppnå en godtagbar skyddsnivå.

Översynen av EU:s regelverk för elektroniska kommunikationer (ELKOM)

Elektroniska kommunikationer är ett av de områden som kommissionen framhåller som EU:s mest framgångsrika. Genom utvecklingen på området har konsumenterna fått större valfrihet, lägre priser och tillgång till nyskapande produkter. Tillväxten är snabbare här än för EU-ekonomin som helhet, och framstegen på området bidrar till att göra hela den europeiska ekonomin mer produktiv och konkurrenskraftig. Den ökade tillgången till kommunika-

tionstjänster hotas dock av tekniska och organisatoriska brister, samt av den mänskliga faktorn. Utvecklingen innebär också att nätverken t sett blir mer öppna och sårbara än tidigare. Det är bland annat därför kommissionen har konstaterat att det nuvarande regelverket för elektroniska kommunikationer måste omarbetas för att förbli effektivt under det kommande årtiondet.[34]

Det EU-regelverk för elektroniska kommunikationer och kommunikationstjänster som nu gäller, består av fem direktiv.[35] Dessa genomfördes i Sverige under 2003, huvudsakligen genom lagen (2003:389) om elektronisk kommunikation.[36] Regelverket tar sikte på att främja konkurrens, konsolidera den inre marknaden för elektronisk kommunikation och gagna konsumenter och användare. När det gäller informationssäkerhet uttrycks kraven i lagtexten dock svagt. Det påtalades som en brist i Informationssäkerhetsutredningens tredje delbetänkande Säker information – Förslag till informationssäkerhetspolitik".[37]

I november 2005 inleddes i EU översynen av regelverket för elektroniska kommunikationer. Syftet med översynen är bland annat att förbättra säkerheten, att konsolidera den inre marknaden samt att stärka konsumenternas och användarnas intressen. Huvudsyftena är dock att kommissionens politik för fördelning av frekvensband ska tillämpas på elektronisk kommunikation, samt att göra det enklare att se över marknader som kan komma i fråga för förhandsreglering.[38]

I juni 2006 presenterades ett meddelande som klargör hur regelverket har fungerat i förhållande till sina mål och vad som bör ändras, samt ett arbetsdokument som beskriver de nya förslagen mer ingående.[39] GD INFSO, som är kommissionens ansvariga generaldirektorat för elektro-

[34] KOM/2006/0334, översynen av EU:s regelverk för elektroniska kommunikationsnät och kommunikationstjänster.
[35] Direktiv 2002/19/EG, 2002/20EG, 2002/21/EG, 2002/22/EG och 2002/58/EG.
[36] Lag (2003:389) om elektronisk kommunikation.
[37] SOU 2005:42, Säker information – Förslag till informationssäkerhetspolitik, s 159.
[38] COM 11190/06, Review of the EU Regulatory Framework for Electronic Communications Networks and Services.
[39] KOM/2006/0334.

nisk kommunikation, förväntas under andra halvåret 2007 presentera ett förslag till direktiv på området.

Som vi nämnde ovan har kommissionen meddelat att informationssäkerhet kommer att utgöra en viktig del av förslaget till ny lagstiftning. Det kom fram i det meddelande och förklarande dokument som har publicerats på området. Det handlar här om att utvidga och stärka de gällande bestämmelserna om säkerhet och nätintegritet, och att dessutom samla dessa i ett särskilt kapitel i det nya ramdirektivet.

Här följer några punkter som enligt planen ska omfattas av det nya direktivet.

- De tekniska och organisatoriska åtgärder som tjänsteleverantörer måste vidta för att skydda sina nät ska regleras mer i detalj. Bland annat föreslås att företag som tillhandahåller elektronisk kommunikation ska bli skyldiga att informera konsumenter om säkerhets åtgärder som kan vidtas vid olika incidenter samt för att förebygga hot och minska sårbarheter.

- Det ska gå att ställa krav på att tjänsteleverantörer vidtar tekniska och organisatoriska åtgärder för att upprätthålla säkerheten i sina tjänster. Kommissionen föreslår bland annat att reglerande myndigheter ska informeras om incidenter som leder till förlust av personliga data eller störningar. Det framhålls också att krav bör kunna ställas på att leverantörer informerar de kunder som förlorar personliga data.

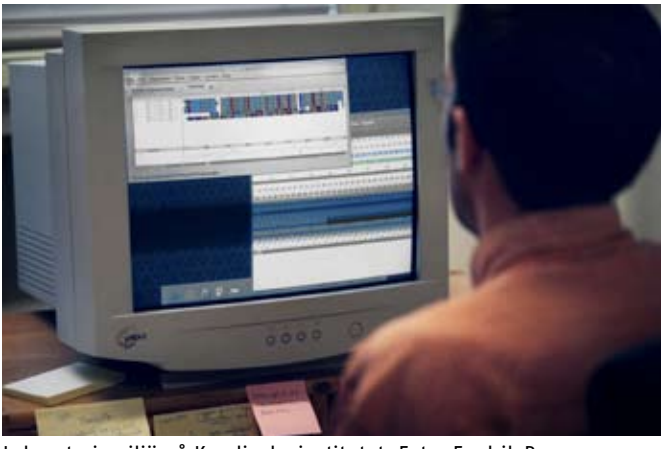
- Det ska gå att ställa krav på att det publika telenätets operatörer utökar integritetsskyddet vid mobila tjänster samt IP-tjänster.

Påverkansmöjligheter

När det pågår en process inom den första pelaren, t.ex. utvecklingen av EPCIP och översynen av ELKOM, är nog möjligheterna att påverka förslagens större drag störst i initiativfasen. Då beslut fattas med kvalificerad majoritet

finns ingen möjlighet att lägga in veto i beslutsfasen. Samtidigt har utvidgningen av EU medfört att det även har blivit svårare att få gehör i beslutsfasen. Det är därför avgörande att samordna sig nationellt tidigt i processen, och lyfta frågan genom seminarier med deltagare från samtliga berörda sektorer. Då de offentliga samråden avslutas är det förmodligen viktigt att skapa sig en samlad bild av förslagen och att synpunkter kan lämnas på sådant som bör ändras eller påverkas längre fram. Om man gör invändningar i ett senare skede finns det risk för att trovärdigheten urholkas om de inte bygger på tidigare argument.

När det gäller informationssäkerhetsfrågor inom processer som EPCIP och ELKOM är det också särskilt viktigt att hitta forum för att utbyta information mellan privat och offentlig sektor. Det beror på att privata företag i stor utsträckning berörs av initiativen. Man kan bygga upp samverkansforum eller utnyttja befintliga forum för att föra upp frågor som hör till arbetet med informationssäkerhet på EU-nivå. Den samverkansgrupp för informationssäkerhet (SAMFI) som KBM har inrättat skulle t.ex. kunna ha en stående punkt om EU på sina möten när intressenter från industri och universitet har bjudits in. t sett är det också viktigt att undersöka vilka medlemsstater som har ungefär samma åsikter i frågan och bygga koalitioner, inför förhandlingar om t.ex. direktivförslag under beslutsfasen.



Laboratoriemiljö på Karolinska institutet. Foto: Fredrik Persson.

När det gäller utvecklingen framåt kan vi dock konstatera att när det gäller informationssäkerhetsaspekterna av EPCIP och ELKOM finns det stort utrymme att påverka även i genomförandefasen. Det gäller nog framför allt EPCIP, eftersom det inom denna process mest handlar om åtgärder som ska understödja annan verksamhet. Det mest avgörande steget i processen framåt på informationssäkerhetsområdet när det gäller EPCIP är troligen därför utvecklingen av de sektorsspecifika kriterierna. Som vi tidigare har nämnt, kommer en genomförandekommitté att fatta beslut om dessa. När det gäller ELKOM har informationssäkerhetsfrågorna varit en del av processen från början i större utsträckning. Trots att det finns stora möjligheter att påverka utvecklingen i genomförandefasen, hamnar nog inte tyngdpunkten på arbetet i denna fas, som när det gäller EPCIP. EPCIP är ett tillfälle för svenska myndigheter att ytterligare föra in krisberedskapsperspektivet i informationssäkerhetsarbetet på EU-nivå.

För båda processerna gäller att det i genomförandefasen måste finnas beredskap för att delta aktivt i syfte att se till att informationssäkerhetsfrågorna får det utrymme de kräver. Det är ju i den fasen som lagstiftningen ska preciseras och mer konkreta regler utformas. Svenska representanter måste ha gedigen kunskap och goda kontakter i Sverige. Slutligen är det viktigt i alla faser av beslutsprocessen att de nationella aktörerna samarbetar för att skapa en enad front och hålla konsekvent linje.

5.2.3 Ökad robusthet

EU-kommissionen finansierar miljöprojekt och transeuropeiska nätverk inom infrastrukturen på transportområdet inom ramen för sina strukturfonder. EU-kommissionen genomför dock ytterst få konkreta åtgärder i egen regi för att öka robustheten när det gäller IKT i befintliga kritiska system. De åtgärder som ska öka robustheten sker i stället i form av normerande processer, som exempelvis programmet för skydd av europeisk kritisk infrastruktur (EPCIP) samt stöd till att utveckla tekniska medel och stöd till studier inom olika program.

Stödet sker exempelvis inom ramen för programmen Prevention, Preparedness and Consequence Managementof Terrorism and other Security related Risks"[40] samt sjunde ramforskningsprogrammet. Från början var det inte meningen att programmen skulle öka robustheten och skydda den kritiska infrastrukturen, men då området visade sig vara så viktigt har det fått visst utrymme inom programmen. Det är ett tecken på att det är möjligt att påverka programmen även i ett senare skede, om de yttre förutsättningarna och det politiska läget tillåter.

Påverkansmöjligheter

För att de kritiska systemen ska bli mer robusta, är det viktigt att agera inom de normerade processerna som har med kritiska infrastrukturer att göra. Det är också viktigt att påverka utformningen i stora program som ramforskningsprogrammet (jfr tidigare och kommande avsnitt).

Det pågår verksamhet för att öka robustheten inom flera olika viljeyttringar. Därför är det viktigt att samordna informationssäkerhetsarbetet nationellt. Då kan man skapa en helhetsbild och prioritera vilka processer som Sverige behöver delta i.

En annan möjlighet för att öka robustheten hos kritiska system inom den europeiska unionen är att arbeta för att strukturfonderna längre fram ska kunna utnyttjas för det ändamålet. Liknande åtgärder inom strukturfonder riktar sig idag till länder där BNP per invånare är lägre än 90 procent av genomsnittet i EU. Det gör att Sverige inte kan ta emot finansiellt stöd.

5.2.4 Samverkan

IKT är ett område där utvecklingen i övriga världen är viktig för EU:s fortsatta tillväxt. För att ta tillvara Europas intressen strävar EU efter att skapa ett starkt samarbete med länder, industrin och forskarmiljön, framför allt

[40] Beslut 2007/125/RIF, inrättande, som del av det allmänna programmet om säkerhet och skydd av friheter, av det särskilda programmet Förebyggande och bekämpande av brott för perioden 2007–2013.

inom EU men även utanför regionen. På så vis får EU tillgång till expertis från ledande aktörer inom olika områden. Ett tätare samarbete med industrin gör det dessutom troligare att satsningarna blir verklighet och utmynnar i resultat som är värdefulla för EU. Värdet är dels tillväxt, dels att säkerheten i området stärks.

När det gäller samverkan mellan EU och industrin har olika industrikonsortier profilerat sig som viktiga aktörer. Ett industrikonsortium är ofta en internationell branschsammanslutning av företag som har gemensamt intresse inom en specifik fråga eller ett område. Konsortiet för industriföretagens gemensamma talan och blir på så vis en tyngre aktör än de enskilda företagen. Konsortiet arbetar för att viktiga beslutsfattare inom ett område ska förstå företagens planer. Vissa industrikonsortier har fått en sådan position och tyngd att medlemsstater väljer att diskutera frågor med konsortiet innan de behandlas inom EU-processerna.

Under EU:s beslutsprocess för EU en dialog med representanter från myndigheter, industrin och forskningsinstitut. Vilka kommissionen samverkar med beror på vad det är för typ av program, och vilka kontakter de ansvariga har. Policyfrågor berör ofta EU:s allmänna utveckling, och företräds av statliga aktörer. Industrin och universitet får en mer framträdande rådgivande roll i frågor som i högre grad berör forskning och utveckling. Samarbetet med experter som inte representerar medlemsstaterna sker framför allt för att inhämta expertutlåtande och synpunkter. Det kan ske via en mängd olika metoder som expertmöten och öppna möten, och berör framför allt initiativfasen i EU:s beslutsprocess.

I takt med att EU har utvidgats har beslutsprocessen blivit allt trögare. Inom informationssäkerhetsområdet upplever kommissionen att bara några av medlemsstaternas representanter kan tillräckligt mycket. För att påskynda processen utnyttjas i stället inofficiella nätverk som består av aktörer med stor insyn i frågan. Dessa aktörer har ett intresse av att arbetet fortskrider. Inom dessa nätverk görs

en viktig del av arbetet som förser de större arbetsgrupperna med material. Vilka aktörer som konsulteras varierar beroende på vilket initiativ det gäller. Det kan t.ex. vara experter från medlemsstater, industrikonsortier eller forskare.

Påverkansmöjligheter

För att Sverige ska kunna delta i och utöva inflytande i EU:samarbetsforum, gäller i princip samma resonemang som för övriga viljeyttringar. Det är viktigt att inte bara veta hur och mot vem man ska agera, utan också att veta när. Genom att skaffa sig kunskap om processinriktningen så tidigt som möjligt, får man förutsättningar att kunna agera. Arbetet blir lättare om Sverige aktivt verkar för att svenska representanter, t.ex. nationella experter, får strategiska positioner inom kommissionen. Det underlättar också om Sverige stödjer aktörer i deras strävan att nå centrala roller i dels den officiella, dels den inofficiella beslutsprocessen.

I Sverige finns det ganska goda kunskaper på området, och Sverige bör därför ha stora möjligheter att spela en central roll när det gäller informationssäkerhetsarbetets inriktning. Det gäller för den officiella beslutsprocessen, men kanske ännu mer för den inofficiella.

De inofficiella kanalerna gör att aktiva medlemsländer eller andra aktörer kan få ett stort inflytande över processen.

EU – parlamentet I Bryssel. Foto: Juha Roininen.

Ofta kan kommissionens val av samverkanspartner inom det inofficiella nätverket te sig något ad hoc. Valet faller ofta på aktörer som kommissionen redan har etablerat en kontakt med, och som bedöms kunna bidra till att stärka processen och föra den framåt. Det är med andra ord centralt att vara aktiv och tillgänglig när tillfällen ges. Har man en gång etablerat kontakt med kommissionen och skapat sig ett gott rykte, ökar sannolikheten att de återkommer i en annan fråga.

En nationell aktör som vill ha maximalt inflytande bör samordna sin verksamhet. På så vis kan Sverige garantera att nödvändig processkunskap och kunskap i sak finns representerad. Om det vid något tillfälle inte går att ordna, är det viktigt att de svenska representanterna får nödvändigt stöd från myndigheter eller regeringskansli. Inom vissa av initiativen är dock detta stöd eftersatt. Det gör att de svenska representanterna får förlita sig på sitt personliga nätverk för att lösa sina problem. Genom att i högre utsträckning samarbeta med nationella aktörer från industrin och universitet kan Sverige på ett effektivare vis utnyttja rikets sammanlagda resurser. Om de svenska aktörerna dessutom samordnar verksamheten och utgår från en gemensam svensk ståndpunkt med tydliga prioriteringar, skapar de en enhetlig linje och därmed bättre förutsättningar för att påverka inriktningen. Både industrin och universiteten har kunskaper i sakfrågor som skapar förutsättningar för att de ska delta i EU-arbetet. Det kan dock vara svårt att som oinvigd i de byråkratiska turerna bidra med råd eller genomföra ansökningar inom programmen. Det är därför viktigt att svenska myndigheter med större erfarenhet av de byråkratiska processerna kan bidra med sådant stöd.

Det är även viktigt med samordning utanför Sverige. Om ett land samarbetar och skapar koalitioner med framför allt mer inflytelserika nationer, har det större chans att få igenom sitt förslag. Det gäller särskilt om de börjar samarbeta tidigt i processen. Därför är det viktigt att vara insatt i andra aktörers inställning i informationssäkerhetsfrågor.

5.2.5 Hantera incidenter

För att incidenter ska kunna hanteras effektivt, måste de relevanta aktörerna ha ett nära samarbete såväl globalt som nationellt. Aktörerna kan bland annat hjälpa varandra genom kunskapsöverföring i fråga om incidenter, risk- och sårbarhetsanalyser och metod- och procedurutveckling. Sedan CERT-funktioner (Computer Emergency Response Team) etablerades i USA har det vuxit fram motsvarande organisationer och sammanslutningar i världen och i Europa. FIRST är ett globalt forum för incidenthanterings- och säkerhetsorganisationer med deltagare från statliga myndigheter, näringslivet och universitet. På europeisk nivå finns det sammanslutningar som TF CSIRT (Task Force Computer Computer Security Incident Response Team) och EGC (European Government CERT:s). Den viktigaste sammanslutningen för Sverige är den informella gruppen EGC, vars syfte är att utveckla effektiv samverkan inom informationssäkerhetsområdet. Inom EGC sker det ett dagligt utbyte av stöd och information.

Inom EU finns det idag inget samarbete med syfte att hantera incidenter eller deras konsekvenser.[41] Inom ramen för EPCIP finns det dock planer på att ta fram ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN) för att underlätta informationsutbyte om gemensamma hotbilder och sårbarheter inom EU. Kommissionen har även i sitt meddelande om en strategi för informationssäkerhet föreslagit att ENISA får en utökad roll.[42] Kommissionen föreslår att en "multilingual information sharing and alert system" skapas vid ENISA. Systemet skulle koppla samman både offentliga och privata aktörers arbete. Kommissionen vill även se att ENISA samlar information om incidenter som redan har inträffat. Medlemsstaterna kommenterade kommissionens meddelande i en resolution från den tolfte december 2006, men lämnade idén om att göra ENISA mer operativt därhän.

[41] Undantaget den incidenthanteringsverksamhet som bedrivs inom ramen för EU:s säkerhets- och försvarspolitik (ESFP).

[42] KOM/2006/251 av den 31 maj 2006 – En strategi för ett säkert informationssamhälle – Dialog, partnerskap och användarinflytande.

ENISA strävar ändå efter att stödja den incidenthanterings-verksamhet som bedrivs inom Europa. Förbehållningen är att de inte ska skapa något dubbelarbete. Det är en svår balansgång då stor verksamhet redan sker parallellt i andra forum sedan mer än ett decennium. ENISA har hittills bidragit inom incidenthantering med kartläggning av befintliga CERT i Europa, ordnat seminarier samt utvecklat en användarmanual för hur man uppför en CERT-funktion. Utöver det utvecklar ENISA sitt kontaktnät med aktörer både inom och utanför Europas gränser

Påverkansmöjligheter

Det finns ett behov av ökad samverkan inom incident-hanteringsområdet, särskilt när det gäller informations-distribution, teknisk kompetens, early warning etc. Det skulle gå att effektivisera verksamheten genom bättre samordning och gemensamma verksamhetsplaner. Om samarbetet ökade skulle det gå att öka specialiseringen mellan de olika länderna inom olika inhämtningsområden och tekniker för en större effekt. I vilken utsträckning EU ska stå för förbättringen av verksamheten är mer oklart. För att Sverige ska kunna påverka diskussioner om huruvida EU ska bli en operativ aktör när der gäller incidenthante-ring, är det viktigt att Sverige följer och aktivt tillämpar de metoder som finns för att utöva inflytande över denna beslutsprocess i EU. Det är också viktigt att bevaka processen för utvecklingen av CIWIN.

5.2.6 Kompetens

Även om ordet kompetens leder tanken till ett ganska brett spektrum av åtgärder, fokuserar vi på forskning i följande analys (i några fall kommer även utvecklingsin-satser att belysas). Vi gör den här avgränsningen eftersom det är forskningsvärlden som växelverkar mest med EU-arenan. Visserligen är ett av ENISA:s verksamhetsteman medvetandehöjande och förtroendeskapande åtgärder, samtidigt som kommissionen genomför medvetande-höjande åtgärder riktade mot internetanvändare inom ramen för programmet Safer Internet plus. Forskning har

dock en mängd beröringspunkter med andra viljeyttringar, t.ex. ökad robusthet och tekniska medel.

Inom EU:s forskningspolitik är det i de allra flesta fall tillväxt som ligger i centrum för intresset. Alltså bedrivs merparten av arbetet inom ramen för det som ibland kallas politik för innovationssystem. Grunden till detta är att hela EU:s forskningspolitik i första hand ses som ett viktigt medel i det som kallas den förnyade Lissabonstrategin för tillväxt och jobb.[43] EU:s forskningspolitik för att uppnå ökad säkerhet samt en utvecklad förmåga till krishantering är ett betydligt mindre utvecklat område än påverkan för innovation och tillväxt.

EU finansierar forskning inom IKT via en rad olika kanaler. Den ojämförligt viktigaste är det just sjösatta sjunde ramprogrammet, som löper mellan åren 2007 och 2013. Utöver det sjunde ramprogrammet finns en rad andra aktiviteter som har med informationssäkerhet att göra. Man bör särskilt framhålla forskning inom skydd av kritisk infrastruktur (EPCIP) som finansieras av GD JLS och den forskning som bedrivs inom ramen för Joint Research Centre (JRC). Utöver detta finns även en del aktiviteter av nätverkskaraktär, bland annat EUREKA som är ett samarbete för att utveckla växelverkan och utbyte mellan företag och forskare i Europa inom mer tillämpad forskning och teknisk utveckling.

Inom det sjunde ramprogrammet ryms IKT inom det tema som kallas ICT Work Programme, med en totalbudget på ungefär 9 miljarder euro. Detta tema är i sin tur uppdelat i sju områden, så kallade Challenges, plus ett specialområde kring framtida omogna teknologier.[44] Det område som mest uttalat berör informationssäkerhet är Challenge 1: Pervasive and trusted network and service infrastructure. I formuleringen av målet för denna forskning, som finansieras av EU, blottläggs tillväxtperspektivet: "The overall goal of Challenge 1 is to enable the emergence of

[43] KOM/2005/24, att arbeta tillsammans för tillväxt och sysselsättning – Nystart för Lissabonstrategin.

[44] http://cordis.europa.eu/fp7/ict/.

network and service technologies that open up new application scenarios and innovative business models, thus creating novel business opportunities and growth."[45] För hela temat ICT utmärker sig följande nyckelord: trusted, secure, privacy, privacy preserving och integrity.

Inom ett av sjunde ramprogrammens teman syns inte tillväxtperspektivet lika tydligt. Det gäller det nyligen lanserade säkerhetstemat. I målen som anges för säkerhetsforskningen handlar det i stället om att utveckla kunskaper och teknologier för att skydda medborgarna från hot som terrorism, organiserad brottslighet, naturkatastrofer och andra olyckor. Detta ska göras med hänsyn tagen till grundläggande medborgliga rättigheter som integritet och rättssäkerhet. Men även här skiner den ekonomiska politiken igenom. Som ett tredje mål för säkerhetsforskningen anges att syftet med forskningsmedlen är att stärka den europeiska "säkerhetsindustrin".[46] Budgeten för tema säkerhet är 1,4 miljarder euro under ramprogrammets hela period.

Tidsförhållandena är mycket långa när EU:s forskningspolitik formas. Det nu aktuella sjunde ramprogrammet började utformas i direkt anslutning till att det tidigare programmet hade beslutats 1999 och initieringen av det sjunde programmet skedde mellan 2002 och 2003.

Skogsbrand, Lissabon 2006. Foto: AFP.

[45] http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html.
[46] http://cordis.europa.eu/fp7/cooperation/security_en.html.

Genomförandefasen består främst av två delar. Man ställer fast så kallade arbetsprogram samt fattar beslut om fördelning av forskningsanslag. Forskningen får sin inriktning genom utformningen av arbetsprogrammen. I dessa fastställs en detaljerad beskrivning av prioriteringar och utvärderingskriterier för delområden inom ramprogrammet. Under ramprogrammets levnad uppdateras arbetsprogrammen flera gånger.

Innehållet i arbetsprogrammen tas fram med hjälp av så kallade Advisory Groups, som består av experter inom aktuella ämnesområden som är utvalda av EU-kommissionen, samt via rådgörande med olika EU-myndigheter. En annan viktig grupp är EURAB (European Research Advisory Board) som kan ses som ett oberoende forskningsråd som har ett antal olika arbetsgrupper för olika områden. Till varje arbetsprogram knyts en programkommitté som godkänner innehållet i arbetsprogrammen.

En viktig påverkansgrupp är IGLO[47] som består av medlemsstaternas och kandidatländernas kontor för bevakning av EU:s ramprogram i Bryssel. För svensk del är det Vinnovas Brysselkontor som är medlem i IGLO. Enligt uppgift är det en inflytelserik gruppering.

Påverkansmöjligheter

EU:s forskningspolitik inom informationssäkerhet är strategiskt relevant eftersom Sverige har intresse av att kunna påverka inriktningen av EU:s forskningspolitik. Ett aktivt agerande gör också att svenska aktörer kan få forskningsmedel från EU. Detta rimmar också väl med den första punkten i informationssäkerhetsutredningens tiopunktsprogram (4.1): "Utveckla Sveriges position inom EU och i (andra) internationella sammanhang".[48]

Då forskningspolitiken innefattar processer som pågår under mycket långt tid är det viktigt att man påverkar där utdelningen kan bli störst. t sett gäller det att man ska påverka tidigt för att nå framgång. En generell nyckelfaktor för framgång är "timing" i påverkansarbetet. Då proces-

[47] http://www.iglortd.org/
[48] SOU 2005:42 s. 10

serna för att forma forskningspolitiken är mycket långa blir det ännu viktigare att veta dels hur och mot vem man ska agera, dels när. Det är därför viktigt att arbeta på ett sådant sätt att man ständigt är beredd på att agera. Det beslutsunderlag som behövs ska finnas till hands när möjligheten kommer. Att börja med att ta fram beslutsunderlag när tillfället upptäcks kan i många fall vara för sent.

Därför är det viktigt att tidigt få kännedom om förändringar. Det kan uppnås genom att svenska representanter får en central roll i arbetsprocessen alternativt genom att nationella experter placeras på strategiskt lämpliga positioner inom kommissionen. Härvidlag är svenskt näringsliv en till stor del bortglömd resurs för att rekrytera kompetenta medarbetare inom EU. Det gäller inte minst inom IKT-området.[49]

I verkligheten sker påverkan genom både formella och informella kanaler. Medlemsstaternas regeringar och deras organ och arbetet i programkommittéerna är de huvudsakliga formella kanalerna för inflytande inom forskningspolitiken. Runt dessa kanaler byggs olika former av informella kanaler upp. Där kan man tidvis uppnå stort inflytande. Det kan vara olika former av intressegrupper (lobbying), enskilda forskare, företag etc. Det är t.ex. relativt vanligt att kommissionen kontaktar samordnare av större EU-projekt för synpunkter kring utformningen av kommande områden inom ramprogrammen eller arbetsprogrammen. En tydlig tendens är att de informella kanalerna vinner mark på bekostnad av de formella beslutsprocesserna.[50]

Enligt Vinnova har Sverige aldrig fullt ut organiserat och prioriterat ett långsiktigt aktivt påverkansarbete på utformningen av EU:s forskningspolitik. Svenska aktörer har inte till fullo insett när man ska påverka eller vem och hur som ska påverkas för att man ska kunna agera samord-

[49] Strategier för svenskt forskningsutbyte på EU-nivå. Område: IT och telekom, Regeringsuppdrag, Vinnova, 2006.

[50] En offensiv roll för Sverige i Europas forsknings- och utvecklingsarbete. Strategier för ökat svenskt utbyte av FoU-program på EU-nivå., Huvudrapport, Regeringsuppdrag, Vinnova (2006) sid. 53.

nat.[51] För att råda bot på detta har Vinnova lagt ett förslag till strategi för ökad påverkan. För studiens syfte är det viktigt att påpeka att Vinnova som utgångspunkt utformar strategin på ett sätt som utgår ifrån "näringslivets behov samt akademiska och industriella styrkeområden."[52] I strategin nämns överhuvudtaget inget om säkerhets- och krisberedskapsperspektivet. I den arbetsgrupp som utformade delstrategin inom it och telekom fanns det inte med någon representant från säkerhetssektorn (KBM, PTS etc.).[53]

Förslaget bygger på att kommittéarbetet delegeras från regeringskansliet till myndigheterna. En beredningsgrupp skapas till varje kommitté. Tanken är att varje beredningsgrupp ska vara det svenska navet gentemot programkommittéernas arbete där olika aktörers EU-strategier utgör utgångspunkter för att forma svenska synpunkter. I förslaget talas det även om en samverkansgrupp som skulle fungera som en nationell arena för att skapa en samordnad svensk påverkan.

En annan del av förslaget inriktas mot att utöka antalet antal svenskar i EU-arbetet, exempelvis nationella experter i arbets- och utvärderingsgrupper. Härvidlag är svenskt näringsliv en till stor del bortglömd resurs för att rekrytera kompetenta medarbetare inom EU. Detta gäller inte minst inom IKT-området.

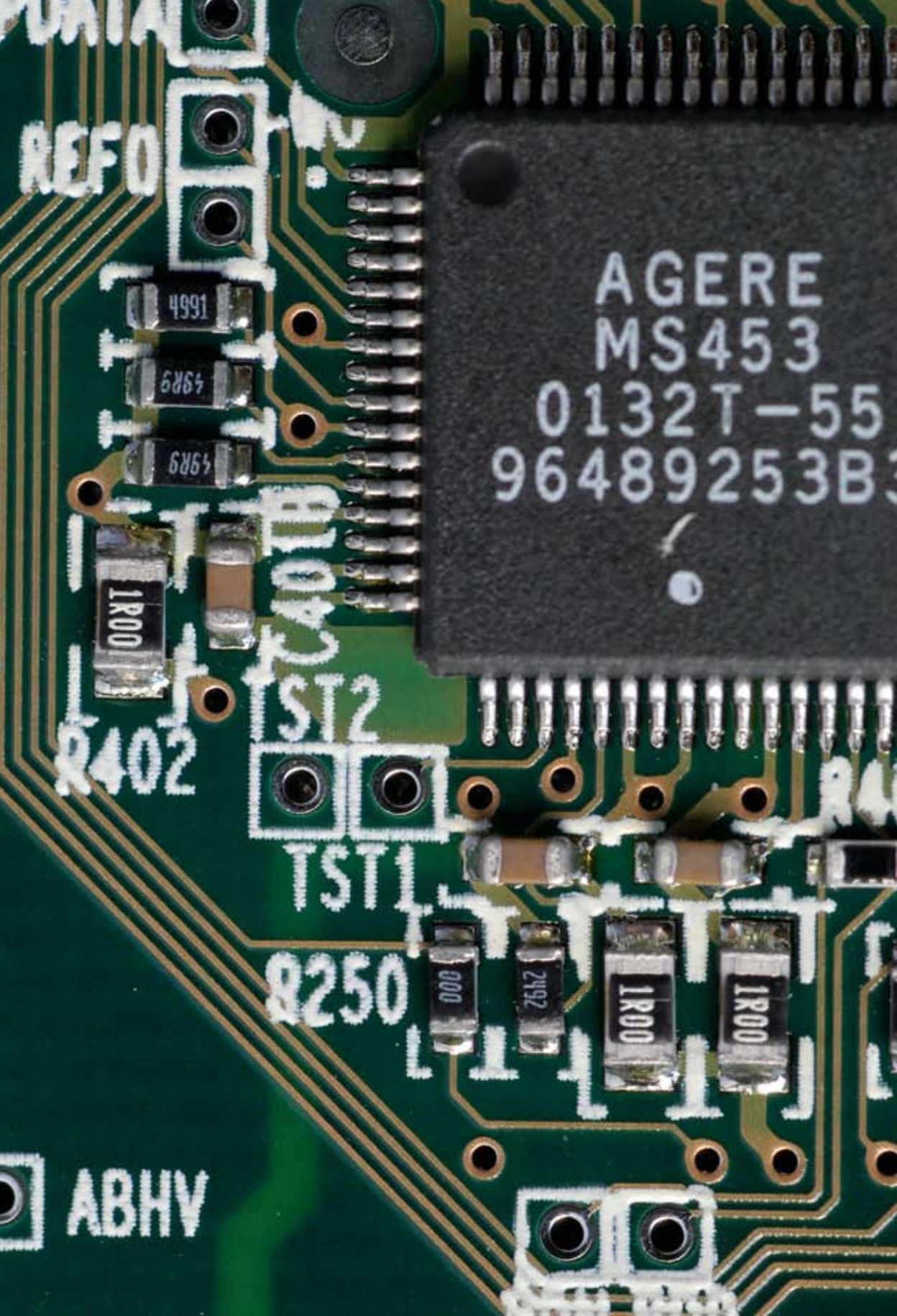
En annan aspekt som är särskilt viktigt för informationssäkerhetsområdet är det upplägg som finns kring avtal med tredje land inom forskningen. Idag finns det en risk för att forskningen blir låst till det nätverk som kommissionen har byggt upp för forskningssamarbete. Inom informationssäkerhet bedrivs en mycket stor del av forsknings- och utvecklingsarbetet utanför EU. USA är en självklar nod och området växer fort i både Indien och Kina.

[51] Vinnova (2006a), s. 10.
[52] Ibid.
[53] Vinnova (2006b), s. 49.

Ett alternativt tillvägagångssätt är att påverka via andra organisationer. En arena för påverkan av EU:s ramprogram är de så kallade European Technology Platforms – ETP. Inom ramen för en ETP samlas en rad aktörer med industriella partner i spetsen för att tillsammans arbeta fram gemensamma visioner och strategier för olika områden. Hittills har ett 30-tal ETP startats, ett flertal inom områden som gränsar till informationssäkerhet. Det är uttalat att dessa plattformar ska agera rättesnöre för att orientera EU:s ramprogram till att passa industrins behov. Idag finns en god svensk representation inom de flesta plattformar med stort IKT-innehåll.[54]

Det finns även andra organisationer och grupperingar som skulle kunna utgöra en god bas för att kanalisera svenska tankar gentemot EU. Exempelvis erbjuder IGLO genom Vinnovas medverkan sådana möjligheter. Eftersom mycket av FoU-aktiviteterna kring informationssäkerhet är av mer tillämpad karaktär torde även EUREKA vara ett intressant forum.

[54] Vinnova (2006b), s. 22.


AGERE
MS453
0132T-55
96489253B
REF0
R402
TST2
TST1
R250
ABHV

6 Slutsatser och åtgärdsförslag

I arbetet med att förbättra det svenska samhällets informationssäkerhet är EU en självklar arena att förhålla sig till. IKT bedöms vara av stor vikt för unionens framtida utveckling och EU flyttar hela tiden fram sina positioner på hela området, informationssäkerheten inräknad. När det gäller informationssäkerhet är EU idag en viktig arena främst när det gäller forskning och teknikutveckling samt normering, d.v.s. olika former av lagstiftning och även till viss del mjukare styrmedel. Det är därför viktigt att Sverige kan utöva ett konstruktivt inflytande på EU:s informationssäkerhetsarbete som gagnar svenska intressen.

EU:s politik inom informationssäkerhetsområdet behandlas inte som ett separat område inom EU:s fördrag. Många olika aktörer deltar i formandet av unionens politik och det finns följaktligen inget samlat arbete på informationssäkerhetsområdet. Sakfrågorna och processerna är utspridda, och den som vill påverka måste övervaka och engagera sig i flera av dem. Av kommissionens generaldirektorat är det främst generaldirektoratet för informationssamhälle och medier (GD INFSO) och generaldirektoratet för rättvisa, frihet och säkerhet (GD JLS) som har viktiga roller i de olika processerna som formar politiken. Enkelt uttryckt ansvarar GD INFSO för forskningsfinansiering medan GD JLS främst ansvarar för polisiärt och straffrättligt arbete. Betydande roller spelar även det gemensamma forskningscentret Joint Research Centre (JRC) och den europeiska nätverks- och informationssäkerhetsbyrån ENISA, den mest renodlade informationssäkerhetsaktören inom EU-strukturen.

Det faktiska arbetet med att utforma politiken görs inom ramen för olika processer. På en övergripande nivå kan alla processer sägas bestå av följande tre faser: initiativfasen, beslutsfasen och genomförandefasen. Den första fasen, initiativfasen, är ofta lång och omfattar alla de

Första fasen:
Initiativfasen

Detalj av moderkortet på en dator.
Foto: Göran Gustafson.

aktiviteter som leder fram till att ett förslag till ny lagstiftning eller ny politik presenteras. I den så kallade första pelaren är det kommissionen som har initiativrätt i denna fas. För att hämta synpunkter från olika aktörer och stärka förslagets legitimitet använder kommissionen en mängd olika metoder. Det handlar här bland annat om konferenser, expertmöten, seminarier och öppna möten. Efter att konsultationstiden har gått ut publiceras oftast alla bidrag eller en analys av resultaten.

Andra fasen: Beslutsfasen

Beslutsfasen inleds då ett förslag till lagstiftning eller annat beslut har presenterats. Det är rådet, d.v.s. medlemsstaternas forum i EU, och i många fall även EU-parlamentet, som tar ställning till förslagen.

Tredje fasen: Genomförandefasen

Den sista fasen, genomförandefasen, är i de flesta fall den längsta av de olika faserna och involverar både kommissionen och medlemsstaterna. Arbetet i denna fas varierar i stor utsträckning beroende på politikområde. Rör det sig t.ex. om lagstiftning inom ramen för ett politikområde i den första pelaren, kan det handla om att precisera lagstiftningen genom att utforma mer konkreta regler och arbetsprogram. Inom EU:s process för forskningsfinansiering handlar genomförandefasen dels om att fastställa så kallade arbetsprogram, dels om att fatta beslut om fördelning av forskningsanslag.

6.1 Påverkansmöjligheter

Inom informationssäkerhetsområdet liksom andra områden är det viktigt att man försöker påverka de delar av processen där utdelningen kan bli störst. En nyckelfaktor för framgång är "timing", det vill säga att vidta åtgärder i rätt ögonblick då det faktiskt är möjligt att påverka utkomsten. För processer inom den första pelaren i allmänhet har man nog störst möjlighet att påverka förslagen i initiativfasen. I och med att EU har utvidgats till 27 medlemsstater är det även svårare att få gehör i beslutsfasen och när beslut fattas med kvalificerad majoritet finns det ingen möjlighet att lägga in veto i beslutsfasen. Det är även viktigt att Sverige för en konsekvent linje. Om

man gör invändningar i ett senare skede finns det risk för att trovärdigheten urholkas om de inte bygger på tidigare argument.

Inom informationssäkerhetsområdet är det dock inte alltid självklart att det är effektivast att påverka verksamheten i ett tidigt skede. Avvägningen kompliceras bland annat av att området är sektorsövergripande, och det faktum att informationssäkerhet är en nödvändig grund för att annan verksamhet ska fungera, snarare än ett eget oberoende område. Följderna blir att informationssäkerhet sällan behandlas inom ett eget initiativ utan i stället integreras i parallella initiativ inom olika politikområden. Detta gör att det blir svårt att få en ordentlig överblick över de olika processerna som är relevanta för informationssäkerhetsområdet. Samtidigt tenderar informationssäkerhetsaspekter att få större utrymme i en senare del av processen och då främst i genomförandefasen. Då blir åtgärderna som behövs för initiativet allt mer konkreta.

Informationssäkerhetsarbetet inom EU bygger alltså på balansgång mellan aktivitet i det initiala skedet för att bevaka att informationssäkerhetsaspekterna behandlas och förs vidare i processen och aktivitet i de senare faserna när informationssäkerhet blir en viktig del av initiativets utformning.

I verkligheten sker påverkan både via formella och informella kanaler. De huvudsakliga formella kanalerna för inflytande är medlemsstaternas regeringar och deras organ och arbetet i programkommittéerna. Den formella arbetsprocessen är dock ganska tungrodd till sin natur och EU:s utvidgning har medfört att det blivit svårare att driva processen framåt. Effektiviteten brister bland annat därför att representanterna i arbetsgrupperna i alltför hög utsträckning är generalister som inte är så insatta i informationssäkerhetsfrågorna. Ibland saknar representanterna dessutom det nödvändiga mandat från hemlandet som de behöver för att föra processen framåt. I stället är deras uppgift främst att bevaka händelseutvecklingen och rapportera till sina överordnade.

För att tillföra den kunskap som behövs och driva processen framåt har kommissionen byggt upp informella kanaler som tidvis kan få stort inflytande. Det kan vara olika former av intressegrupper, enskilda forskare, företag, experter från medlemsstaterna etc. Dessa grupper utför mycket av det arbete som tillför det material som den formella processen behöver för beslut i de olika faserna. Det är t.ex. relativt vanligt förekommande att kommissionen kontaktar de som samordnar större EU-projekt för synpunkter kring hur kommande områden inom ramprogrammen eller arbetsprogrammen ska utformas.

6.2 Åtgärdsförslag

En generell nyckelfaktor för framgång är "timing" i påverkansarbetet. Det är viktigt att känna till hur och i förhållande till vem man ska agera, men det är också viktigt att veta när. Det är därför angeläget att arbeta på ett sådant sätt att man ständigt är beredd att agera. Projektgruppen har tagit fram ett antal strategiska åtgärdsförslag som även har följts av förslag på konkreta åtgärder för hur Sverige i närtid skulle kunna agera för att påverka EU:s informationssäkerhetsarbete. Dessa åtgärdsförslag bedöms vara särskilt relevanta att överväga inför ordförandeskapet i EU hösten 2009. Som en konsekvens av ordförandeskapet har Sverige då ett utmärkt tillfälle att påverka EU:s informationssäkerhetsagenda. I detta sammanhang bör nämnas att den kanske allra största möjligheten att påverka förmodligen finns inom ramen för översynen av det sjunde ramforskningsprogrammet. Översynen ska ske under hösten 2009. Åtgärderna är till sin form beroende av varandra och därför presenterar vi dem nedan utan inbördes rangordning.

Bli en central och aktiv aktör

För att få inflytande över EU:s informationssäkerhetsarbete är det viktigt att vara en central aktör inom både de officiella och de inofficiella processerna. Om man fungerar som en naturlig rådgivande kontakt för EU:s institutioner har man chans att få lämna förslag som ligger i linje med

Sveriges intresse. En annan fördel med att förfoga över representanter som har stor insyn i utvecklingen av EU:s informationssäkerhetsarbete är att man då kan upptäcka förändringar i ett tidigt skede. Därmed kan man vidta nödvändiga åtgärder.

Sverige kan skapa förutsättningar för att bli en central och aktiv aktör genom att svenska representanter genom goda arbetsinsatser bygger upp ett förtroende inom EU:s institutioner så att dessa förlitar sig allt mer på deras råd och arbetsinsatser. Detta kan dock ta resurser från andra verksamheter i anspråk.

Det kan vara en mödosam process att bygga upp ett tillräckligt förtroende för att bli en central aktör. Eftersom Sverige är en av de medlemsstater som har stor kunskap i de här frågorna finns en god bas för att landet ska kunna bli en central aktör. Dessutom tyder våra intervjuer på att kommissionen var välvilligt inställd till aktörer som var villiga att hjälpa till med att föra arbetet framåt. Att bidra aktivt kan dock ta mycket tid i anspråk, vilket riskerar att ske på bekostnad av annan verksamhet inom informationssäkerhetsområdet. Svenska informationssäkerhetsmyndigheter skulle kanske gemensamt kunna stödja utvalda representanter. På så vis får de mindre arbetsbörda, och fler aktörer kan tillgodogöra sig resultatet.

Ett annat sätt att skapa förutsättningar för att bli en central aktör inom EU:s informationssäkerhetsarbete är att uppmuntra rekryteringen av svenska funktionärer inom området och rekommendera tillsättningen av nationella experter på strategiskt lämpliga positioner inom kommissionen (och eventuellt inom ENISA). Härvidlag utgör svenskt näringsliv och universitet en intressant resurs och den offentliga sektorn skulle kunna sprida information om tjänsterna samt uppmuntra kompetenta personer att söka.

Koordinera och prioritera de svenska insatserna

Som liten medlemsstat måste Sverige välja vilka frågor och processer man aktivt ska försöka påverka. Det är därför

nödvändigt att prioritera bland ansträngningarna för att påverka EU:s informationssäkerhetsarbete. För att kunna prioritera rimligt är det av central betydelse att ha en klar bild av vilka pågående processer som är relevanta för informationssäkerhet. Därtill är det viktigt att det finns en grund för en gemensam svensk ståndpunkt, och att samtliga svenska aktörer känner till den. Ett sådant underlag gör det lättare att prioritera och underlättar för en liten aktör som Sverige att samordna resurser och skapa en enad front utåt för att få så stort inflytande som möjligt. Handlingsplanen är en god grund för den svenska ståndpunkten. Men för att kunna arbeta flexibelt är det viktigt att den svenska ståndpunkten utvecklas och förtydligas allt eftersom arbetet i EU fortgår. Det är viktigt att de svenska aktörerna samarbetar i fråga om utvecklingsarbetet.

En utökad diskussion kring aktuella EU-frågor i befintliga forum skulle också kunna bidra till att skapa en gemensam utgångspunkt för EU-arbetet. Det är därmed avgörande att tidigt i processen samordna sig nationellt och lyfta frågan genom samråd och seminarier med deltagare från samtliga berörda sektorer. För att skapa en överblick över de pågående processerna skulle ett gemensamt e-forum kunna utvecklas i anslutning till de samverkansforum som finns idag.

I det här sammanhanget är det också av central betydelse att länken mellan myndigheterna som arbetar med informationssäkerhetsfrågor och behörigt departement byggs upp. Ett sätt kan vara att i större utsträckning bjuda in departementsföreträdare till olika diskussions- och samverkansforum, samt att etablera kontakten genom att ha möten några gånger per år.

Skapa en kunskapsbas för agerande inom EU:s informationssäkerhetsarbete

För att de svenska aktörerna på informationssäkerhetsområdet ska kunna utöva inflytande är det viktigt att de skaffar sig såväl breda som djupa kunskaper om EU:s informationssäkerhetsarbete. Det räcker inte med enbart sakkunskaper. De måste också känna till andra aktörers

inställning samt skaffa sig kunskaper om själva processen och hur de bör agera i alla dess faser.

Breda kunskaper kan man skaffa sig genom exempelvis självstudier av relevant litteratur och handböcker samt genom att delta i kurser av övergripande karaktär. Dessa kan i ett senare skede kompletteras med seminarier med fokus på aktuella processer och sakfrågor i syfte att skapa förutsättningar även för djupare kunskaper. Djupare kunskaper kan man skaffa sig genom att delta i befintliga nationella samverkans- och diskussionsforum. Till exempel skulle SAMFI på sina möten kunna gå igenom aktuella EU-frågor med koppling till informationssäkerhet som en stående punkt på agendan.

Det är också viktigt med processkunskap, d.v.s. kunskaper om hur EU:s politik utformas och implementeras. Detta för att öka medvetenheten kring hur påverkan sker via dels formella, dels informella kanaler. Även här kan kurser bidra till större förståelse för de processer som formar beslut och andra former av initiativ. Men det är minst lika viktigt att ordna "studiebesök" i Bryssel för de aktörer som inte får en naturlig inblick i det praktiska arbetet

Utnyttja samtliga nationella resurser i samhället

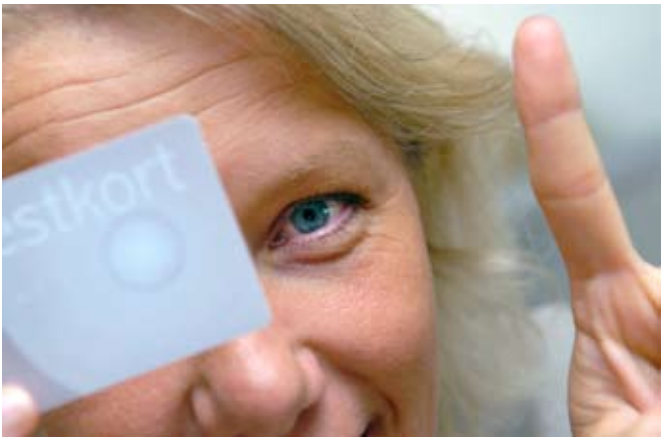
Syftet med EU:s arbete inom utveckling av tekniska medel är till stor del att skapa förutsättning för tillväxten inom unionen. Därmed har EU och industrin ett gemensamt intresse av att industrin deltar aktivt i processen. Svensk industri och svenska universitet har mycket att tillföra i form av sakkunskap och har därmed stora möjligheter att bidra. Genom att utveckla samarbetsformer mellan industrin, universitet och offentliga aktörer kan synergier uppnås. Ett tätare samarbete med industrin och samordning av verksamhet kan bidra till att resurser utnyttjas mer effektivt, samtidigt som man skapar en mer enad front utåt.

För att underlätta samarbetet kan Sverige anordna seminarier i aktuella ämnen, och bjuda in representanter från myndigheter, departement, näringsliv och universitet.

Man skulle t.ex. kunna diskutera informationssäkerhetsaspekter inom det sjunde ramforskningsprogrammet eller ett relevant tema för i2010-konferensen under ordförandeskapet

Påverka via allianser och andra organisationer

Genom att inleda samarbeten med andra aktörer i ett tidigt skede av processen, och gemensamt föra arbetet framåt, kan man lättare nå framgång. Att bygga koalitioner med andra medlemsstater är ett sätt att skapa större tyngd bakom förslagen. Ett alternativt tillvägagångssätt är att påverka via andra organisationer och konsortier för att kanalisera svenska ståndpunkter gentemot EU. Exempelvis erbjuder IGLO genom Vinnovas medverkan sådana möjligheter. Eftersom mycket av FoU-aktiviteterna kring informationssäkerhet är av mer tillämpad karaktär är förmodligen även EUREKA ett intressant forum. Ytterligare en arena för påverkan av EU:s ramprogram är det som kallas för European Technology Platforms (ETP). Inom ramen för en ETP samlas en rad aktörer med industriella partner i spetsen för att tillsammans arbeta fram gemensamma visioner och strategier för olika områden, där ett flertal områden gränsar mot informationssäkerhet. Det är uttalat att dessa plattformar ska agera rättesnöre för att orientera EU:s ramprogram till att passa industrins behov.



Charlotte Rosengren-Edgren är ansvarig för SAS biometriprojekt på Umeå flygplats. Vid en biometrisk kontroll jämför en dator ögats iris med en bild på ett ID-kort. Foto: Krister Larsson

Sverige borde vidmakthålla och utveckla det svenska deltagandet inom dessa forum. Det är dock viktigt att den svenska verksamheten inom dessa forum stämmer överens med det svenska prioriterings- och koordineringsarbetet.

Öka insatserna för att påverka EU:s forskningspolitik

Eftersom tillväxtperspektivet idag är så starkt, finns det en tendens att det kommer att dominera formandet av EU:s forskningspolitik, tillsammans med de akademiskt inriktade delarna. För att kunna lyfta fram kompletterande mål för politiken, exempelvis ökad säkerhet, bör svenska aktörer inom krisberedskapssystemet försöka påverka utformningen av EU:s forskningspolitik. Det är i detta sammanhang viktigt att understryka att forskning inom informationssäkerhet finansieras via en rad olika EU-program. Därför är det viktigt att undvika en inlåsning enbart kring EU:s säkerhetsforskning

EU-Medlemsländer 2007.

Källförteckning

Offentligt tryck

SOU 2003:27, *InfoSäkutredningen, delrapport 1 om signalskydd*.
SOU 2004:32, *Informationssäkerhet i Sverige och internationellt – en översikt, Delrapport 2 från InfoSäkutredningen*.
SOU 2005:42, *Säker information – förslag till informationssäkerhetspolitik, delbetänkande om InfoSäkutredningen*.
SOU 2005:71, *Utredningen om informationssäkerhetspolitik – organisatoriska konsekvenser, Slutbetänkande från InfoSäkutredningen*.
Proposition 2001/02:158 *Samhällets säkerhet och beredskap*.
Proposition 2006:133 Samverkan vid kris – för ett säkrare samhälle.
Lag (2003:389) *om elektronisk kommunikation*.

EU-dokument

KOM/2007/285 *av den 1 juni 2007 om utvärderingen av den europeiska byrån för nät- och informationssäkerhet (ENISA)*.
KOM/2007/146 *slutlig av den 30 mars 2007 om i2010 – Årsrapport om informationssamhället 2007*.
KOM/2006/0787 *slutlig av 12 december 2006 om förslag till Rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna*.
KOM/2006/0688 a*v den 15 november 2006 om skräppost, spionprogram och sabotageprogram*.
KOM/11190/06 *Communication from the Commission on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services*.
KOM/2006/0334 *av den 29 juni 2006 om översynen av EU:s regelverk för elektroniska kommunikationsnät och kommunikationstjänster*.
KOM/2006/251 *av den 31 maj 2006 – En strategi för ett säkert informationssamhälle – Dialog, partnerskap och användarinflytande*.
KOM/2005/576 *av den 17 november 2005, grönbok om ett europeiskt program för skydd av kritisk infrastruktur*.
KOM/2005/229 *av den 1 juni 2005 om i2010 – Det europeiska informationssamhället för tillväxt och sysselsättning*.
KOM/2005/121 *slutlig av den 6 april 2005, förslag om upprättande av ett ramprogram för konkurrenskraft och innovation (2007–2013)*.
KOM/2005/24 *av den 2 februari 2005, Att arbeta tillsammans för tillväxt och sysselsättning – Nystart för Lissabonstrategin*.
KOM/2001/0298, *Nät och informationsstrategi – Förslag till en europeisk strateg.i*
Beslut 2007/125/RIF *av den 12 februari 2007 om inrättande, som del av det allmänna programmet om säkerhet och skydd av friheter, av det särskilda programmet Förebyggande och bekämpande av brott för perioden 2007–2013*.
Beslut 1639/2006/EG *av den 24 oktober 2006 om att upprätta ett ramprogram för konkurrenskraft och innovation 2007–2013*.

Beslut 854/2005/EG *av den 11 maj 2005 om inrättandet av ett flerårigt gemenskapsprogram för att främja en säkrare användning av Internet och ny online-teknik*.

Beslut 2006/215/EG a*v den 15 mars 2006 om inrättande av en expertgrupp på hög nivå för rådgivning till Europeiska kommissionen om genomförande och utveckling av strategin i2010*.

Direktiv 2002/77/EG *av den 16 september 2002 om konkurrens på marknaderna för elektroniska kommunikationsnät och kommunikationstjänster*.

Direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

Direktiv 2002/22/EG a*v den 7 mars 2002 om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster*.

Direktiv 2002/21/EG a*v den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster*.

Direktiv 2002/19/EG *av den 7 mars 2002 om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter*.

Direktiv 95/46/EG *om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter*.

Förordning 460/2004/EG *av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet*.

EU-kommissionens årliga rapport om den digitala ekonomin – *I2010, 2nd annual report, IP/07/453 – Bryssel den 30 mars 2007*.

eEurope – *An Information Society For All, Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000*.

Litteratur

Fylkner, M., Barck-Holst, S., Englund L., och Jarlsvik, H. (2006) *Vem gör vad inom EU?* – informationssäkerhetsfrågorna i fokus [KBM:s temaserie | 2006:5].

Jönsson, T., och Jarlsvik, H (2005) *Krisberedskapsmyndigheten och Europeiska unionen* [FOI-R–1654–SE].

Eriksson, P. (2004) *Kartläggning av EU:s informationssäkerhetsarbete i första respektive andra pelaren*, [FOI Memo].

Krisberedskapsmyndighetens lägesrapport 2007 – *samhällets informationssäkerhet*.

Esterle, A., Ranck, H. och Schmitt, B. (2005), *Information security – A new challenge for the EU*, [Chaillot Paper Nr. 76].

Nilsson, Maria (2003) *Europeisk säkerhets- och försvarspolitik – En studie av svenska möjligheter att påverka* [FOI-R-0898-SE].

SIS, (2004) Teknisk rapport, handbok 550 utgåva 2: *Terminologi för informationssäkerhet*.

Vinnova (2006) Regeringsuppdrag, *Huvudrapport, En offensiv roll för Sverige i Europas forsknings- och utvecklingsarbete. Strategier för ökat svenskt utbyte av FoU-program på EU-nivå*.

Vinnova (2006) Regeringsuppdrag, *Strategier för svenskt forskningsutbyte på EU-nivå – Område: IT och telekom*.

Intervjuer

Intervju med *tjänsteman vid SITIC*
Intervju med *tjänsteman vid FMV*
Intervju med *tjänsteman vid Vinnova*
Intervju med *tjänstemän vid VERVA*
Intervju med *tjänstemän vid näringsdepartementet*
Intervju med t*jänsteman vid EU-representationen*
Intervjuer med funktionärer vid generaldirektoratet för informationssamhället och medier
Intervju med funktionär vid generaldirektoratet för rättvisa, frihet och säkerhet
Intervju med funktionär vid generaldirektoratet för informationsteknik
Intervju med funktionär vid generaldirektoratet för energi och transport
Intervju med *funktionär vid EU Joint Situation Centre (SITCEN), Rådet*
Intervju med *funktionär vid Department sensitive informationssystem, Rådet*


Bilaga 1

Bilaga 1 – Kartläggning av svenska viljeyttringar

I Sverige pågår arbete för att utveckla och precisera Sveriges viljeyttringar inom informationssäkerhetspolitik. En viktig stötesten är Krisberedskapsmyndighetens pågående regeringsuppdrag att ta fram en svensk handlingsplan för informationssäkerhet. Handlingsplanen baseras på informationssäkerhetsutredningen (SOU 2005:42, SOU 2005:71).

Projektet har analyserat propositionerna (2001/02:158, 2005:133), informationssäkerhetsutredningen (SOU 2005:42 och SOU 2005:71) samt Krisberedskapsmyndighetens lägesrapport 2007 för att identifiera de svenska prioriteringarna inom informationssäkerhetsområdet.

Resultatet ger inte svaret på vilka strategiska prioriteringar Sverige ska göra på nationell eller internationell nivå. Det ligger utanför projektets mandat. Resultatet är en grund för att effektivare kunna identifiera och precisera relevanta EU-processer och aktörer.

Resultatet består av en sammanställning av prioriterade områden. De övergripande målen med informationssäkerhet är att öka förtroendet för it (även tillväxtfrämjande), skydda samhällsviktig verksamhet och grundvärden samt öka integritetsskyddet.

Därutöver har vi inom projektet kategoriserat de svenska viljeyttringarna i sju områden: ökning av robustheten, normering, samverkan, hantering av incidenter, tekniska medel och kompetens. Se tabell nedan.

Ökning av robustheten[55]	Normering	Samverkan	Hantering av incidenter	Tekniska medel	Kompetens
Identifiera säkerhetsbrister	Staten ansvarar för spelregler	Öka samverkan off-privat	Hantera, ingripa, agera för kontinuitet i systemet	Distribution av korrekt tid	Utveckla beställar-kompetens
Fokusera på samhällsviktig verksamhet	Utveckla det författ-ningsmässiga stödet	Ökad samverkan inom det offentliga	Analysera it-störningar	Säker e-ID	Öka säkerhets-medvetandet
	Betydelsen av standarder	Underrättelse-delgivning	Upptäcka it-störningar	Nät för samhällsv. verksamhet	Kryptologisk kompetens
		Öka internatio-nellsamverkan	Incident-rapporterings-funktion	Signalskydd	Säkerställa expertkomp. inom infosäk.
			Återställa		Forskning/om-världsanalys

Tabell: kategorisering av svenska viljeyttringar i verksamhetsområden

Referenslista

På motstående sida följer en referenslista som beskriver i vilka källor som vi har funnit viljeyttringarna. Referenslis-tan ger även en sidhänvisning.

Teckenförklaring:
P X = den strategiska punkten X
S XY = sida XY
Kap Y = kapitel Y

[55] Tidigare: reducera sårbarhet (tekniskt)

Område	Viljeyttringar	SOU 42	SOU 71	KBM 07	Prop. 133
Öka förtroende för it	Säkerställ förtroendet för IKT-system	P2		1	
Öka integritetsskyddet		P2			90
Hantera incidenter					
	Hantera, ingripa, agera för kontinuitet i systemet	P4			90
	Analysera it-störningar	P4,6		3,4	90
	upptäcka it-störningar	P4,6		3,4	90
	Org. system för infosäk. som garanterar kontinuitet	S88			
	Hantera incidenter när de inträffar	S84		5,7	90
	Incidentrapporteringsfunktion		X	4	
	Återställa samhällsviktiga verksamheter				93
Samverkan					
	Förbättra spridning av underrättelseinformation	P5		4	
	Öka den internationella samverkan	P1, s91			
	Ökad samverkan inom det offentliga	P7			
	Ökad samverkan offentligt–privat	S18			
Skydda samhällsviktig verksamhet/Öka robustheten	Fokusera på samhällsviktig verksamhet	P8, s87			
	Identifiera säkerhetsbrister i samhällsviktig verksamhet	S88			
Kompetens	Öka säkerhetsmedvetandet	P9		8	89
	Säkerställa expertkompetensförsörjningen	P10			89
	Beställarkompetens				
	Forskning/omvärldsanalys				
	Kompetensfrågor	Kap 8			
Normering					
	Det författningsmässiga stödet bör utvecklas	S85		3	90
	Staten ansvarar för spelregler	S89			
	Harmonisering av lagstiftning	S91			
	Betydelsen av standarder			13	
Tekniska medel					
	Nät för samhällsviktig verksamhet	Kap 4.2.2		14	
	Säker e-identifiering			2	
	Signalskydd	SOU 2003:27		2	

Bilaga 2

Bilaga 2 – Definitioner

Sverige saknar en officiell definition av informationssäkerhet, men en definition som ofta åberopas och som användes av informationssäkerhetsutredningen[55] är SIS informationssäkerhetsdefinition: "[Informationssäkerhet är] 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"[56]

Motsvarande definition inom EU torde vara definitionen för nät- och informationssäkerhet:

"[Nät- och informationssäkerhet är] förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten (autentisering), integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät"[57].

EU:s definition är konkretare till sin karaktär och inriktar sig på förmågan hos ett nät i stället för att beröra informationstillgångar i allmänhet. Att det finns väsentliga skillnader mellan de olika definitionerna bedöms dock få minimala konsekvenser för det praktiska arbetet mellan Sverige och EU i fråga om informationssäkerhet.

[55] SOU 2004:32 Informationssäkerhet i Sverige och internationellt – en översikt. Delrapport 2 från InfoSäkutredningen, sidan 17

[56] SIS HB 550 utgåva 2 – terminologi för informationssäkerhet, sidan 8.

[57] KOM/2001/0298 sXX "Nät och informationsstrategi – Förslag till en europeisk strategi",.


Bilaga 3

Bilaga 3 – Statliga aktörer

Det svenska arbetet inom informationssäkerhet är uppdelat på och återfinns inom olika politikområden. Hur ansvaret är fördelat beror på vilken sektor som äger den huvudfråga där informationssäkerhetsaspekter har uppkommit som delmoment. Det innebär att frågorna såväl hanterings- som ansvarsmässigt faller på departement och myndigheter inom olika sektorer. De departement som berörs mest är Näringsdepartementet, Finansdepartementet och Försvarsdepartementet.

Enligt ansvarsprincipen är alla myndigheter skyldiga att se till att den egna verksamheten har en tillräckligt hög informationssäkerhet. Sedan finns det myndigheter som arbetar mer direkt med informationssäkerhetsfrågor och ansvarar för vissa delområden. Det finns dock ingen myndighet som har ett utpekat ansvar för att leda och samordna informationssäkerhetsfrågor. Myndigheterna som tar en mest aktiv del i informationssäkerhetsarbetet är Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Post- och telestyrelsen (PTS), Krisberedskapsmyndigheten (KBM), Försvarsmakten (FM), Verket för förvaltningsutveckling (VERVA), Rikskriminalpolisen (RKP) och Säkerhetspolisen (Säpo). Datainspektionen, PTS och Finansinspektionen har dessutom visst tillsynsansvar inom sina respektive område. Här nedan beskriver vi de ovanstående myndigheterna och deras verksamhet inom informationssäkerhet.[58]

[58] För en utförligare beskrivning av de svenska statliga aktörerna inom informationssäkerhetsområdet hänvisas exempelvis till utredningen om informationssäkerhetspolitik – organisatoriska konsekvenser (SOU 2005:71).

Krisberedskapsmyndigheten (KBM)

KBM har ett sammanhållande myndighetsansvar för samhällets informationssäkerhet i Sverige och ska genomföra omvärldsbevakning inom ramen för det arbetet.[59] KBM ska främja utvecklingen av samverkan mellan stat och näringsliv samt vara Sveriges kontaktpunkt för informationssäkerhetsfrågor inom sitt ansvarsområde. I syfte att samordna det nationella arbetet har KBM därför inrättat en samverkansgrupp för informationssäkerhet (SAMFI) där myndigheter med informationssäkerhetsansvar deltar. I SAMFI representeras myndigheterna KBM, PTS, FRA, FMV, FM, Verva, RPS och Säpo. KBM administrerar utöver SAMFI även ett informationssäkerhetsråd.

Försvarets materielverk (FMV)

FMV ska anskaffa, vidmakthålla och avveckla materiel och förnödenheter på uppdrag av Försvarsmakten.[60] Utöver att säkerställa att Försvarsmakten investerar i säkra och robusta system har FMV etablerat en självständig enhet, Sveriges certifieringsorgan för it-säkerhet (CSEC), som ansvarar för uppbyggnad, drift och förvaltning av ett system för utvärdering och certifiering av it-säkerhet i enlighet med standarden ISO/IEC IS 15408 (Common Criteria).[61]

Försvarets radioanstalt (FRA)

FRA ska bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger.[62] I verksamheten ingår även att stödja informationssäkerhetsarbetet hos myndigheter och statligt ägda bolag. Detta kan exempelvis ske genom it-säkerhetsanalyser och genom att hjälpa till med att identifiera inblandade aktörer vid it-relaterade hot mot samhällsviktiga system.[63]

[59] Förordning (2002:518) med instruktion för KBM; http://www.notisum.se/rnp/sls/lag/20020518.HTM
[60] Förordning (1996:103) med instruktion för Försvarets materielverk; http://lagen.nu/1996:103
[61] FMV CSEC http://www.fmv.se/WmTemplates/Page.aspx?id=269#
[62] Förordning (1994:714) med instruktion för FRA; http://www.notisum.se/rnp/sls/lag/19940714.htm
[63] http://www.fra.se/infosak.shtml

Post- och telestyrelsen (PTS)

PTS har en viktig funktion inom informationssäkerhetsområdet genom att myndigheten bär ansvaret för området elektronisk kommunikation.[64] Det avser krav på funktion samt integritetsskydd i elektronisk kommunikation och bidrar till att skapa en robustare infrastruktur. PTS utövar också tillsyn och utfärdar certifikat till allmänheten enligt lagen om kvalificerade elektroniska signaturer. PTS har etablerat Sveriges it-incidentcentrum (SITIC).[65] SITIC bedriver operativ omvärldsbevakning och ska sammanställa och ge ut statistik, sprida information om nya hot mot it-system samt ge råd om förebyggande åtgärder.

Polisen

Inom polisen är det främst Säkerhetspolisen och Rikskriminalpolisen som verkar på informationssäkerhetsområdet. RKP har en egen sektion som hanterar it-brott och RKP driver tillsammans med Säpo en samordningsfunktion för brottsrelaterade it-incidenter (S-BIT).

Försvarsmakten (FM)

Försvarsmakten leder och samordnar signalskyddstjänsten inom totalförsvaret. FM ansvarar för utveckling och godkännandet av signalskyddssystem, produkter för och distribution av signalskyddsnycklar samtidigt som de kontrollerar och följer upp verksamheten. FM utövar dessutom totalförsvarets Certificate Authority (CA) för public key infrastructure (PKI-funktioner). FM utövar i praktiken rollen som National Communication Security Authority (NCSA) samt National Authority (NA) genom den militära underrättelse- och säkerhetstjänsten (MUST), men något formellt beslut existerar inte.

[64] Förordning (1997:401) med instruktion för PTS; http://www.notisum.se/rnp/sls/lag/19970401.HTM

[65] http://www.sitic.se/index.html

Datainspektionen

Datainspektionen är en förvaltningsmyndighet som har till uppgift att skydda människors privatliv i IKT-samhället, bland annat utifrån personuppgiftslagen

Verket för förvaltningsutveckling (VERVA)

Verva har fått regeringens uppdrag att leda och samordna statsförvaltningens utvecklingsarbete med säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar. Verva har till uppgift att skapa bättre villkor och lägre kostnader för den offentliga förvaltningens anskaffning och användning av varor och tjänster på it- och teleområdet.

KBM:s utbildningsserie

2008:3 Crisis Communications Handbook
2008:2 Large scale Internet attacks
2008:1 Sveriges beredskap mot nätangrepp
2007:4 Rätt i kris – Rätt juridiskt och etiskt vid mötet med medier i kriser och olyckor
2007:3 Krisberedskap och sekretess – informationsdelning mellan företag och offentlig sektor
2007:2 Utvärdering av övningar – En handbok för utvärdering av stabs- och beslutsövningar
2007:1 Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar
2006:2 Risk- och sårbarhetsanalyser. Vägledning för kommuner och landsting
2006:1 International CEP Handbook. Civil Emergency Planning in the NATO/EAPC-Countries
2005:1 Medvind i säkerhetsarbetet
2004:1 Trossamfundens medverkan i krishantering
2003:8 Risk- och sårbarhetsanalyser – Introduktion för kommuner
2003:7 Sant eller falskt? Metoder i källkritik
2003:6 Nyheter vid kriser
2003:4 Crises Journalism – A guidance for government agencies
2003:3 Krisjournalistik – En introduktion för myndigheter
2003:1 Crisis Communication Handbook
2002:1 Åsk- och regnoväder över Orust – tusen och åter tusen frågor

ISSN 1652–3539

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08 593 710 00
Fax 08 593 710 01

kbm@kbm-sema.se

www.krisberedskaps
myndigheten.se