Vem gör vad inom EU?

INFORMATIONSSÄKERHETSFRÅGORNA I FOKUS

Malin Fylkner, Svante Barck-Holst,
Linda Englund & Helén Jarlsvik

KBM:S TEMASERIE | 2006:5

KRISBEREDSKAPS
MYNDIGHETEN

KBM:S TEMASERIE | 2006:5

Vem gör vad inom EU?

INFORMATIONSSÄKERHETSFRÅGORNA I FOKUS

Malin Fylkner, Svante Barck-Holst,
Linda Englund & Helén Jarlsvik

Titel: Vem gör vad inom EU? Informationssäkerhetsfrågorna i fokus
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Ablestock
Övriga foton: Sid 16 futureimagebank, sid 35 futureimagebank,
sid 46 Ablestock, sid 63 Ablestock

ISSN: 1652-2915
ISBN: 91-975934-0-0
KBM:s dnr: 1262/2005
Grafisk form: AB Typoform

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning.
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se
KBM:s temaserie 2006:5

Innehåll

Förord 5

Sammanfattning 7

Summary 12

Inledning 17
Bakgrund 17
Studiens syfte och målgrupp 18
Disposition 18

Studiens upplägg, metod och avgränsningar 20
Övergripande upplägg – en schematisk presentation 20
Metodologiska överväganden och avgränsningar 22
Övrigt underlag 28
Projektgrupp 28

Introduktion till EU 29
Inom vilka områden bedriver EU politik? 29
Vilka är EU:s centrala aktörer? 30
Hur ser EU:s politiska beslutsprocess ut? 31
Vad blir resultatet av EU:s politik? 33
Hur berörs svenska myndigheter av EU:s politik? 34

Informationssäkerhet i Sverige och EU – begrepp i fokus 36
Nät- och informationssäkerhet enligt EU:s definitioner 36
Svensk begreppssyn 38
Skillnaden mellan teori och praktik – vilka begrepp gäller? 38

De stora dragen – aktiviteter och initiativ av relevans **39**
Policyutveckling 39
Legala och icke-regulativa ramverk 42
Initiativ kopplade till forskning och utveckling (FoU) 43

Vem gör vad? Aktörer i fokus **47**
EU-kommissionen 47
Rådet 56
Europaparlamentet 57
Myndigheter 58
Decentraliserade organ 59
Övriga aktörer 61

Diskussion och slutsatser **65**
Informationssäkerhet – en fråga som skär genom hela samhället 65
Politik för tillväxt respektive politik för säkerhet 66
Resultatet av EU:s arbete inom informationssäkerhetsområdet 68
Stora möjligheter till medverkan och påverkan för svenska aktörer 69

Förslag till vidare studier **72**
Resultat? En studie om lyckade initiativ och förkastade förslag 72
Allierad eller fiende? En studie om att identifiera gemensamma intressen 72
Att välja väg eller hur påverka internationellt som liten aktör? 73
EU:s interna informationssäkerhetsarbete påverkar Sverige 74
Att mäta nyttan med EU:s arbete – en fallstudie 74
Sverige en strategisk aktör på EU-arenan - hur? 75

Referenser **76**

Förord

Informationssäkerhet har seglat upp som en viktig fråga för aktörer på både nationell och internationell nivå. Till sin karaktär är frågorna såväl sektors- som gränsöverskridande vilket gör hanterandet av dessa frågor till en gemensam angelägenhet. I Sverige har IT-relaterade hot och sårbarheter samt hanterandet av de problem som följer av det moderna samhällets IT-beroende studerats under ett flertal år. Ett antal olika offentliga utredningar har bidragit till viktiga insikter och förslag till nya organisatoriska lösningar och ansvarsfördelningar. Senast (år 2005) var det Informationssäkerhetsutredningen (Fö 2002:06) som levererade sitt slutbetänkande avseende den svenska informationssäkerhetspolitiken och dess organisatoriska konsekvenser.

I InfoSäkutredningens slutbetänkande tydliggörs behovet av att utveckla Sveriges position inom EU och i andra internationella sammanhang. Enligt InfoSäkutredningen bör Sverige ta tillvara möjligheten att bidra till harmonisering av informationssäkerhetsarbetet mellan EU:s medlemmar och spela en aktiv roll i det internationella arbetet.

Sedan början av december 2005 har Totalförsvarets forskningsinstitut (FOI) genomfört en studie om EU och informationssäkerhet på uppdrag av Krisberedskapsmyndigheten (KBM). Den ska ses som ett led i en strävan att förbättra möjligheterna för svenska aktörer att både delta i och påverka informationssäkerhetsarbetet på en europeisk nivå. Förhoppningen är att resultaten av studien ska fungera som en plattform för vidare studier och ett aktivt svenskt agerande inom frågeområdet.

Studien har bedrivits i projektform med deltagande projektmedlemmar från både FOI och KBM. Projektets kärna har utgjorts av Malin Fylkner och Svante Barck-Holst, båda FOI, med bidrag från Linda Englund, KBM. Projektet resulterade i denna rapport och den bifogade cd-skivan. Huvudförfattare till rapporten är Malin Fylkner, FOI. Övriga projektmedlemmar har bidragit i varierande utsträckning med allt från kommentarer till värdefullt underlag, analyser och textskrivningar.

Helén Jarlsvik, FOI, har författat kapitlet *Introduktion till EU*. Ansvarig för den cd-skiva som medföljer rapporten och den presentation av kartläggningsstudien som där återfinns i grafisk form är Svante Barck-Holst, FOI.

Malin Fylkner
Projektledare

I detta arbete har även Linda Englund, KBM, deltagit.

Ett stort tack avslutningsvis till alla de som bidragit till studiens genomförande!

Sammanfattning

Informationssäkerhetsproblematiken är sektoröverskridande och gränsöverskridande, något som gör hanterandet av frågorna till en nationell och internationell angelägenhet. Som en effekt av gemensamma IT-relaterade sårbarheter och i viss mån delade hotbilder ser vi i dag en framväxt av olika initiativ – i Europa och i resten av världen – där informationssäkerhetsrelaterade frågor står i fokus för samverkan mellan olika aktörer.

I takt med att dessa initiativ blir fler och samarbetet mer komplext blir det också allt viktigare för Sverige att delta i och påverka det fortsatta arbetet inom informationssäkerhetsområdet, även utanför landets gränser. För att uppnå detta krävs en fördjupad förståelse för vilka som är de centrala aktörerna på den internationella arenan, hur de fattar beslut och inte minst hur deras inbördes ansvarsförhållanden ser ut. Detta är även viktigt för att kunna tillgodogöra sig resultatet av det internationella arbetet – något som i sin tur ofta kräver anpassning från svensk sida.

Den studie om EU och informationssäkerhet som Totalförsvarets forskningsinstitut (FOI) har genomfört på uppdrag av Krisberedskapsmyndigheten (KBM) – och som slutrapporteras i och med denna rapport – ska ses som ett led i en strävan att förbättra möjligheterna för svenska aktörer att verka i och påverka informationssäkerhetsfrågor på en europeisk nivå. Det övergripande syftet med studien har varit att kartlägga de aktörer inom EU som arbetar med informationssäkerhetsfrågor.

Informationssäkerhet är ett komplicerat begrepp. Dess mångfacetterade karaktär gör att man måste ta hänsyn till både tekniska och administrativa aspekter (ofta definieras begreppet utifrån dessa två komponenter) och att i stort sett alla verksamheter i samhället berörs av frågeställningarna. Inom EU finns det i dag åtskilliga begrepp med prefixet ”e”, exempelvis: eHealth, eGovernance, eSignatures, eCustoms, e-Services, eDefence etc. Dessa begrepp har tydliga informationssäkerhetsrelaterade komponenter. Som exempel kan begreppet eHealth nämnas där bl.a. sekretessaspekter kopplade till digitaliseringen av patientjournaler är frågor av relevans för informationssäkerhetsområdet.

Med tanke på den mångfacetterade sakfrågan är informationssäkerhet en fråga som berör många olika aktörer. Inom EU innebär detta att relevanta frågeställningar återfinns inom ett flertal av den *Europeiska kommissionens generaldirektorat*, där de mest tongivande kan sägas vara generaldirektoratet för informationssamhälle och media (DG InfSo) samt generaldirektoratet för rättvisa, frihet och säkerhet (DG JFS). Eftersom den verksamhet som EU-kommissionen bedriver har sin motsvarighet inom *Europeiska rådet* återfinns även här informationssäkerhetsrelaterade frågor på olika aktörers bord. Exempelvis finns det ett antal rådsarbetsgrupper där informationssäkerhetsfrågorna behandlas (nämnas kan exempelvis den sektorövergripande arbetsgruppen mot organiserad brottlighet och arbetsgruppen för forskning). Utöver dessa aktörer så arbetar även olika *myndigheter* och *decentraliserade organ* med frågorna. Det förstnämnda fallet kan exemplifieras med Enisa, Europeiska byrån för nät- och informationssäkerhet och det sistnämnda med Europol och dess ”High Tech Crime Unit” (HTCC). Till detta ska läggas ett stort antal *intresseorganisationer* (och lobbyorganisationer), *forskningsinstitut* (som inte specifikt behandlas i denna studie men ändå bör nämnas) och *privata aktörer*.

Inom EU styrs ansvarsfrågan till stor del av vilket politikområde som frågan har koppling till och inom vilken pelare detta politikområde har sin hemvist. Lite förenklat kan man säga att informationssäkerhetsfrågorna inom EU kan delas in i två politiska huvudspår – ett där slutmålet är tillväxt och ett där säkerhet i sig står i fokus. Inom det förstnämnda spåret återfinns säkerhetsaspekter kopplade till informationssamhällets utveckling och som berör frågor av social, ekonomisk och teknisk karaktär. Här finns också initiativ kopplade till bl.a. eEurope-arbetet.[1] Till den andra kategorin hör säkerhetsaspekter med bäring på försvarsfrågor, såsom utvecklandet av EU:s militära informationsoperationskoncept och aspekter som mer kopplas till brottslighet, som exempelvis EU-kommissionens rambeslut om angrepp mot informationssystem. Här återfinns även det nu pågående arbetet med att ta fram ett europeiskt program för skydd av kritisk infrastruktur (EPCIP).

Den tydligaste ansvarsgränsen är den mellan första och tredje pelarens verksamheter.[2] Förenklat skulle man kunna uttrycka detta som att informationssäkerhetsfrågor som inte har någon koppling till brottslighet faller inom första pelaren, medan frågor med IT-brottsförtecken hamnar inom den tredje pelaren. Vid våra intervjuer i Bryssel framkom att generaldirektoratet för

1. eEurope 2002, eEurope 2005, i2010, m.fl. Se vidare i avsnittet *Policyutveckling*.
2. Av projektets avgränsningar följer att verksamheten inom 2:a pelaren inte prioriterats. Detta medför att analysen fokuserats kring verksamhet hemmahörande i första respektive tredje pelaren.

informationssamhälle och media samt generaldirektoratet för rättvisa, frihet och säkerhet sinsemellan gjort en uppdelning av de frågor som generaldirektoratet ska ansvara för i enlighet med denna pelarindelning.[3] Enligt uppgifter faller frågor kopplat till cyberterrorism, Critical Infrastructure Protection (CIP) och cyberbrottslighet på DG JFS och cybersäkerhet (strategi) på DG InfSo. Noteras bör att även om dessa två generaldirektorat fördelat ansvaret sinsemellan på nämnda vis finns det andra aktörer som också arbetar med frågor kopplade till dessa områden. Exempelvis är generaldirektoratet för energi och transport högst inblandat i arbetet med det europeiska programmet för skydd av kritisk infrastruktur (EPCIP).

Som konstaterats ovan finns det ett stort antal aktörer inom EU som på ett eller annat sätt berörs av eller ”ansvarar för” informationssäkerhetsfrågorna. Vilket är då det konkreta resultat som kommer ur EU:s arbete inom informationssäkerhetsområdet? På en övergripande nivå kan man prata om *strategiska policyinitiativ* som en form av resultat. Dessa återfinns inom såväl området politik för säkerhet som politik för tillväxt, vilka båda nämnts tidigare. I det förstnämnda fallet finns initiativ kopplade till exempelvis kampen mot terrorism (där även CIIP- och CIP-frågor berörs) och i det sistnämnda bl.a. de så kallade eEurope-initiativen (där säkerhet som en ”tillväxtmotor” utgör en naturlig och viktig del).

Ett annat resultat är de *direktiv och förordningar* som kommer ur EU:s processer och vars innehåll i sin tur styr det fortsatta arbetet, både på en europeisk nivå och i de enskilda medlemsstaterna. Kopplat till informationssäkerhetsområdet finns det ett stort antal relevanta direktiv och förordningar. Några exempel, tematiskt sorterade:

- *Nät och informationssäkerhet:* Förordning 460/2004/EG om inrättandet av den europeiska byrån för nät- och informationssäkerhet.
- *Cyberbrottslighet och terrorism:* Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet, KOM 2000/890.
- *Integritet och skydd av personuppgifter:* Direktivet om integritet och elektronisk kommunikation 2002/58/EG.
- *Skydd av kritisk infrastruktur och CIIP:* Grönbok om ett europeiskt program för skydd av kritisk infrastruktur, KOM 2005/0576.[4]

3. I stället för ansvar kan man prata om att ”ta ledningen” (engelska ”lead”) inom ett område eftersom det formellt sett inom EU inte är så att ett enskilt generaldirektorat kan ”äga” en fråga. När exempelvis ett meddelande arbetats fram och beslutats, är det EU-kommissionen som helhet som står bakom det, inte ett enskilt generaldirektorat.
4. För en mer omfattande genomgång av relevanta direktiv och förordningar samt förslag se avsnitt *Legala och icke regulativa ramverk.*

Skapandet av *nya organisatoriska enheter*, som Enisa, kan ses som ett annat och väldigt påtagligt resultat av EU:s arbete.

Till detta ska läggas den *forskningsrelaterade verksamhet* som EU bedriver och de resultat som denna verksamhet utmynnar i. Det finns ett stort antal forskningsprojekt av relevans för informationssäkerhetsområdet som antingen har finansierats alternativt finansieras via EU-medel. Många projekt som finansieras via ramforskningsprogrammen leder till nya tekniska lösningar som kan sägas utgöra frukterna av EU:s långsiktiga arbete med att säkerställa unionens tekniska innovationskraft.

Slutligen bidrar EU:s arbete till att bygga upp och underhålla *nätverk* mellan europeiska aktörer. EU:s processer är uppbyggda på ett sätt där konsultativa inslag utgör en viktig grund. Här kan exempelvis EU-kommissionens arbete nämnas, och den konsultativa fas som ofta inleder arbetet kring en ”ny” fråga. EU kan även välja att vidta nätverksbefrämjande åtgärder som att skriva in uttryckliga krav på interoperabilitet och kommunikation mellan olika aktörer inom ramen för specifika program.

Detta sagt om EU:s aktörer och resultatet av det arbete som bedrivs inom unionens ramar. Men vilka förutsättningar har de svenska aktörerna att medverka i och påverka EU:s arbete? Vår slutsats är att svenska aktörer har en stor möjlighet att både delta i och påverka EU:s arbete inom informationssäkerhetsområdet – och även att uppnå viktiga resultat. Det finns exempel på ”EU-vana” aktörer som redan i dag aktivt medverkar i och påverkar det som sker inom EU, men motsatsen existerar också. Det är vår bedömning att Sverige borde kunna använda sin befintliga kunskapsbas och de existerande nätverk och kontaktytor mellan svenska aktörer och deras europeiska motsvarigheter på ett mer strategiskt och koordinerat sätt. Ökad nationell samordning skulle kunna ge bättre effektivitet och ökat genomslag i detta sammanhang.

Det är viktigt att känna till att det i regel krävs mer av ett mindre land (som Sverige får sägas vara i EU-sammanhang) för ett framgångsrikt agerande. Förutom ett större deltagande och en högre grad av engagemang krävs även sakkompetens, kunskap om hur EU fungerar och slutligen ”vänner”. Att skapa en förståelse för hur andra länder ställer sig i enskilt viktiga frågor och hur deras hållning i dessa frågor svarar mot svenska intressen är avgörande för att identifiera aktörer med vars hjälp det går att uppnå en hävstångseffekt inom EU. Ovanstående är främst skrivet med svenska myndigheter i åtanke, men gäller till stor del för andra aktörer också.

Avslutningsvis leder en studie som denna oundvikligen till intressanta uppslag och idéer kring behov av vidare studier. I rapportens slutkapitel presenteras några av dessa uppslag lite närmare, men nedan följer några rubriker som är tänkta att inspirera till fortsatt läsning:

- Resultat? En studie om lyckade och förkastade förslag

- Allierad eller fiende? En studie om att identifiera gemensamma intressen
- Att välja väg, eller hur kan en liten aktör påverka?
- EU:s interna informationssäkerhets-arbete påverkar Sverige
- Att mäta nyttan med EU:s arbete – En fallstudie
- Sverige en strategisk aktör på EU-arenan – Hur?

Summary

Information security problems cut across sectors and borders, and managing these issues is both a national and international concern. Due to common IT-related vulnerabilities, and to a certain degree of shared threat scenarios, we now see initiatives – across Europe and the rest of the world – where information security-related issues provide a basis for collaboration between different stakeholders.

As the number of initiatives increases and collaboration becomes more complex, the importance of Sweden taking part in and contributing to continued work in the information security area also increases, even beyond its own national boundaries. Achieving this goal requires an in-depth understanding of who the most important stakeholders are in the international arena, how they make decisions and not least, their mutual accountability. It is also important to benefit from the results of this international work – which often requires adaptation from a Swedish perspective.

This study – and final report – on the EU and Information Security was carried out by the Swedish defence Research Agency (FOI) on behalf of the Swedish Emergency Management Agency (SEMA). It should be seen as a step towards improving opportunities for Swedish stakeholders to take part and influence information security issues at a European level. The overall purpose of the study has been to identify the stakeholders who work with information security issues within the EU.

Information security is a complex concept. The diversity of this area requires consideration of both technological and administrative aspects (a definition of the concept is often based on these two components) and the problems affect almost all facets of society. Several EU concepts bear the "e" prefix: eHealth, eGovernance, eSignatures, eCustoms, eServices, eDefence, etc. All of these concepts have obvious information security-related components. Information security is, for example, a major issue in the eHealth sector where confidentiality and the digitalization of patient information are high on the agenda.

As such, information security affects a wide range of stakeholders. In the EU, information security issues are handled by several European Commission Directorate-Generals, in particular the Directorate-General for Information Society and Media (DG InfSo) and the Directorate-General for Justice, Freedom and Security (DG JFS). As the Commission and the European Council conduct similar activities, information security issues also appears on several other agendas. A number of official working groups are active in the area (the Multidisciplinary Group on Organised Crime and the research workinggroup, for example) and a number of agencies and decentralised bodies also focus on these issues. These include the European Network and Information Security Agency (Enisa), and Europol and its "High Tech Crime Unit" (HTCC). There are also a large number of interest and lobby groups, research institutes (that are not treated specifically in this study but still deserve a mention) and private stakeholders.

Responsibility in the EU is determined to a large degree by the policy area in question and its relevant pillar. Briefly, information security issues in the EU can be divided into two main political categories – one that focuses on growth, the other on security. The first-named category includes security aspects pertaining to developments in the information society that are influenced by social, financial and technological issues. This also includes initiatives connected to the "eEurope" work. The other category contains security aspects pertaining to defence issues, such as development of the EU's information operation concept, and aspects that are more related to crime, such as the Commission's framework decision on attacks against information systems. This also includes ongoing work to develop a European Programme for Critical Infrastructure Protection (EPCIP).

The clearest delineation of responsibilities lies between the activities of the first and third pillars. Briefly, information security issues with no connection to crime fall under the first pillar, while issues related to computer crime fall under the third pillar. Our interviews in Brussels showed that the Directorate-General for Information Society and Media (DG InfSo) and the Directorate-General for Justice, Freedom and Security (DG JFS) had divided their own areas of responsibility according to these pillar divisions. Issues related to cyber terrorism, Critical Infrastructure Protection (CIP) and cyber crime fell under the auspices of DG JFS, while DG InfSo handled issues related to cyber security (strategy). It should also be noted that even though these two Directorate-Generals divided their responsibilities in this manner, other stakeholders are also active in these areas. For example, the Directorate-General for Energy and Transport is heavily involved in efforts to develop a European Programme for Critical Infrastructure Protection (EPCIP).

As mentioned above, many stakeholders in the EU are in some way affected or responsible for information security issues. What then are the concrete results that EU work will produce in this area? At overall level, one could say that strategic policy initiatives are one form of result. These appear in both security and growth policies, both of which are mentioned above. The first-named includes initiatives related to combating terrorism (which also concern CIIP and CIP issues) and the latter includes eEurope initiatives (where security as a "growth engine" constitutes a natural and important component).

Another result is the directives and regulations that come from EU processes, of which the contents steer continued work at both European level and in individual member states. A large number of directives and regulations are relevant in the information security area. Some examples, sorted thematically, include:

- *Network and information security:*
  Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
- *Cyber crime and terrorism:*
  Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM 2000/890.
- *Integrity and protection of personal data:*
  Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- *Protection of critical infrastructure and CIIP*:
  Green Paper on a European programme for critical infrastructure protection, COM 2005/0576.

The creation of new organizational units such as Enisa is another concrete result of EU work.

Added to this are the research-related activities run by the EU and the results they produce. Many of the research projects that are relevant in the information security area either have been or are currently financed by the EU. A number of projects financed by the framework programmes have led to new technological solutions that can be seen as the fruits of long-term EU work aimed at securing the Union's technological innovativeness.

Finally, EU work contributes to building and maintaining networks between European stakeholders. Consultative features form an important part of EU processes. The work of the Commission is a good example, as is the consultative phase that usually precedes work with "new" issues. The EU can also choose to introduce network strengthening measures such

as specifying requirements for interoperability and communication between different stakeholders within the framework of specific programmes.

This describes EU's stakeholders and the results of work carried out within the Union's frameworks. But what opportunities exist for Swedish stakeholders to take part and influence the EU's work? Our conclusion is that Swedish stakeholders can both take part and influence EU work in the information security area – and make important contributions. There are several examples of "experienced" EU stakeholders who already participate actively and contribute to what happens in the EU, but the opposite is also true. Our assessment is that Sweden could use its current knowledge base and the networks and contact surfaces that already exist between Swedish stakeholders and their European counterparts in a much more strategic and coordinated manner. Increased national coordination would boost effectiveness and impact in this context.

It is important to understand that a smaller country (such as Sweden in this context) usually has to work harder to achieve results. Besides greater participation and a higher degree of involvement, the relevant expertise, knowledge of how the EU works and finally "friends" are also important. Creating an understanding of how other countries position themselves on specific issues and how this corresponds to Swedish interests is essential for gaining leverage in the EU. This applies particularly to Swedish authorities, but also to other stakeholders.

To conclude, a study like this inevitably leads to interesting proposals and ideas around the need for further studies. Some of these suggestions are studied in more depth at the end of the report, but the following headings are included to inspire further reading:

- Results? A study of successful and rejected proposals
- Friend or foe? A study on how to identify joint interests
- Choosing a direction, or how small stakeholders can also make a difference
- How the EU's internal information security work affects Sweden
- Measuring the added value of EU work – A case study
- Sweden, a strategic player in the EU level – How?

Inledning

Bakgrund

Att informationssäkerhetsproblematiken är transnationell och således en fråga som inte kan lösas enbart på en nationell nivå är inget nytt. I åratal har det betonats, i olika sammanhang, att det är viktigt att få till stånd ett gränsöverskridande samarbete. Detta är nödvändigt för att komma till rätta med de problem som följer av den ökande grad av ”IT-fiering” som genomsyrar vårt samhälle, men även för att kunna dra nytta av de möjligheter som följer med den nya tekniken. Vi ser i dag ett antal olika initiativ på europeisk och internationell nivå där frågor kring informationssäkerhet står i fokus för samverkan mellan olika aktörer.[5] I takt med att initiativen blir fler och samarbetet mer komplext blir det också allt viktigare för Sverige att delta i och påverka det fortsatta arbetet inom informationssäkerhetsområdet – även utanför vårt lands gränser.

I InfoSäkutredningens slutbetänkande tydliggörs behovet av att utveckla Sveriges position inom EU och i andra internationella sammanhang. I den föreslagna strategin för informationssäkerhet formuleras detta som en viktig punktsats. Enligt InfoSäkutredningen bör ”Sverige ta tillvara möjligheten att bidra till harmonisering av informationssäkerhetsarbetet mellan EU:s medlemmar och spela en aktiv roll i det internationella arbetet”.[6] Detta uttrycks i liknande ordalag i propositionen ”Samverkan i kris – för ett säkrare samhälle”. I den anser regeringen att ”Informationssäkerhet är ett gemensamt, internationellt problem och att strategiska lösningar måste utvecklas i samverkan med andra länder, både inom EU och internationella organ”.[7]

För att kunna delta i och påverka arbetet med informationssäkerhets-

5. Initiativ med bäring på informationssäkerhetsområdet har bl.a. tagits inom ramen för FN:s säkerhetsråd, OECD, G8 m.fl.
6. InfoSäkutredningens slutbetänkande SOU 2005:71, ”Informationssäkerhetspolitik, organisatoriska konsekvenser”, sid. 89.
7. Proposition 2005/06:133: ”Samverkan i kris – för ett säkrare samhälle”, sid. 90.

frågor på en internationell nivå krävs en fördjupad förståelse för vilka som är de centrala aktörerna, hur de fattar beslut och inte minst hur deras inbördes ansvarsförhållanden ser ut. Detta är även viktigt för att kunna tillgodogöra sig resultatet av det internationella arbetet – något som i sin tur ofta kräver anpassning från svensk sida. I dag saknas viktiga komponenter för att nå denna förståelse. Den bild som finns är fragmenterad och otydlig vilket gör det svårt för de svenska aktörerna att spela en aktiv roll i internationella sammanhang.

Den studie om EU och informationssäkerhet som FOI sedan början av december 2005 har genomfört på uppdrag av KBM – och som slutrapporteras i och med denna rapport – ska ses som ett led i en strävan att förbättra möjligheterna för svenska aktörer att verka i och påverka informationssäkerhetsfrågor på europeisk nivå. Förhoppningen är att resultaten av studien ska fungera som en plattform för vidare studier och ett aktivt svenskt agerande inom frågeområdet.

Studiens syfte och målgrupp

Det övergripande syftet med studien har varit att kartlägga de viktigaste aktörerna inom EU när det gäller informationssäkerhetsrelaterade frågor. Ambitionen har varit att försöka skapa en initial grund för att svenska aktörer med relevant verksamhet bättre ska kunna förhålla sig till de europeiska organen, både för att kunna tillgodogöra sig resultatet av EU:s arbete, men även för att kunna påverka utvecklingen av detsamma.

Studiens målgrupp utgörs huvudsakligen av läsare insatta i frågor som rör informationssäkerhet och som vill ha en guide till EU:s arbete inom området, snarare än läsare som är kunniga om EU och önskar fördjupa sig i informationssäkerhetsfrågor.

Följande frågeställningar har varit av central betydelse för studien och dess genomförande:

- Vilka aktörer inom EU arbetar med informationssäkerhet eller relaterade frågor?
- Hur ser ansvarsförhållandena mellan EU:s institutioner ut när det gäller informationssäkerhetsfrågorna?
- Hur ser processerna ut kring EU:s politik på området? Vilka aktörer är tongivande i dessa processer?
- Hur ser de befintliga kontaktytorna och relationerna mellan svenska (främst myndighetsrelaterade) och europeiska aktörer ut i dag?
- Vilken möjlighet till informationsutbyte och påverkan finns för svenska aktörer i EU:s processer?

Disposition

I kapitlet *Studiens upplägg, metod och avgränsningar* redovisas hur studien genomförts, bakomliggande metodansatser och överväganden, viktiga

avgränsningar och begrepp som är centrala för studien. Detta kapitel ger en bakgrund till studien och viktiga ingångsvärden för att kunna värdera de resultat som presenteras i rapporten.

I det nästföljande kapitlet finns en översiktlig beskrivning av EU där nedanstående frågor står i fokus:

- Inom vilka områden bedriver EU politik?
- Vilka är EU:s institutioner?
- Hur ser EU:s beslutsprocesser ut?
- Vad blir resultatet av EU:s politik?
- Hur involveras svenska myndigheter i EU:s arbete?

Syftet med detta kapitel är att skapa förståelse hos de läsare som inte arbetar med EU utan som i stället har sin huvudsakliga kompetens inom informationssäkerhetsområdet. För de mer EU-initierade läsarna kan detta kapitel lämnas därhän.

Kapitlet *Informationssäkerhet i Sverige och EU – Begrepp i fokus* tar avstamp i de olika begreppsmässiga uppfattningar som finns i Sverige och i Europa. Kapitlet, som mer är av bakgrundskaraktär, syftar främst till att ge svenska aktörer insyn i de definitioner och begrepp som man i EU-sammanhang använder sig av för att på så vis skapa goda förutsättningar för agerande.

Under rubriken återfinns en översiktlig genomgång av de viktigaste linjerna i det arbete som bedrivits kopplat till informationssäkerhetsområdet under de senaste åren. I detta kapitel, liksom kapitlet *Vem gör vad? Aktörer i fokus* presenteras resultatet av kartläggningsstudien, med fokus på just aktörsfrågan.

Kartläggningsmaterialet i rapporten kompletteras av ett presentationsmaterial i form av en elektronisk karta gjord med hjälp av mindmapping-teknik i programmet Mindjet MindManager®. Detta material återfinns på den cd-skiva som bifogas rapporten.

Kartan åskådliggör komplexa organisatoriska kopplingar och innehåller dessutom

- beskrivningar av olika aktörers verksamhet och sakfrågor
- relevanta dokument (direktiv, meddelanden, presentationer etc.)
- länkar till dokument, kontaktinformation och information som de olika aktörerna själva publicerat på Internet m.m.

Kartan är sökbar och syftet är att den ska underlätta för den som snabbt vill navigera till rätt aktörer eller till specifik information kopplad till informationssäkerhetsområdet.

I kapitlet *Diskussion och slutsatser* presenteras generella insikter som studien genererat och som bedömts vara relevanta för de aktörer – främst myndigheter – som har som strategiskt mål eller ansvar att agera i EU-sammanhang. Några av de frågor som adresseras är: Hur påverkar man policyutvecklingen inom EU? Vad krävs? Vad kan man som enskild aktör åstadkomma?

Slutligen presenteras i kapitlet *Förslag till vidare studier* tankar kring några områden som det skulle vara givande att studera vidare.

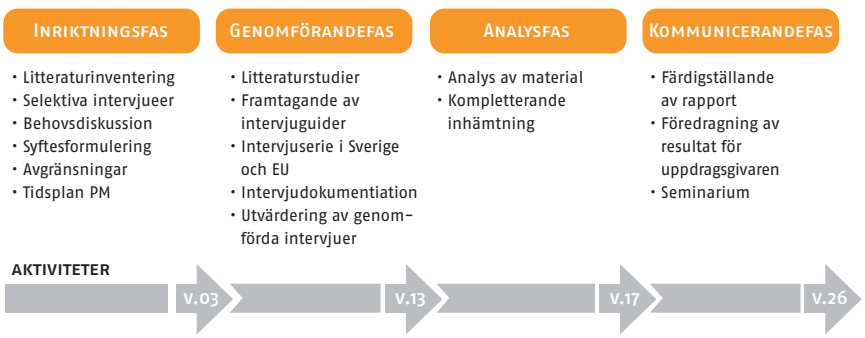
Studiens upplägg, metod och avgränsningar

Övergripande upplägg – en schematisk presentation

Nedan presenteras en schematisk bild över studiens upplägg. De viktigaste faserna är tydligt markerade och förklaras utförligare nedan.

Inriktningsfas

Inriktningsfasen av studien syftade till att skapa en förståelsegrund för att kunna formulera relevanta frågeställningar att arbeta vidare med. En stor del av detta arbete genomfördes av projektgruppen under december 2005 och utmynnade i den inriktningspromemoria[8] som låg till grund för det fortsatta arbetet. Relevant litteratur inventerades, intervjuer genomfördes med personer med insyn i frågeområdet, metodologiska aspekter som avgränsningar, urval av studieobjekt m.m. diskuterades (se nedan).



Figur 1. *Övergripande upplägg.*

8. FOI Memo 1614, (2005), ”Studie om informationssäkerhet i EU – En precisering av studiens syfte, avgränsningar, metod och material”, Malin Fylkner och Svante Barck-Holst.

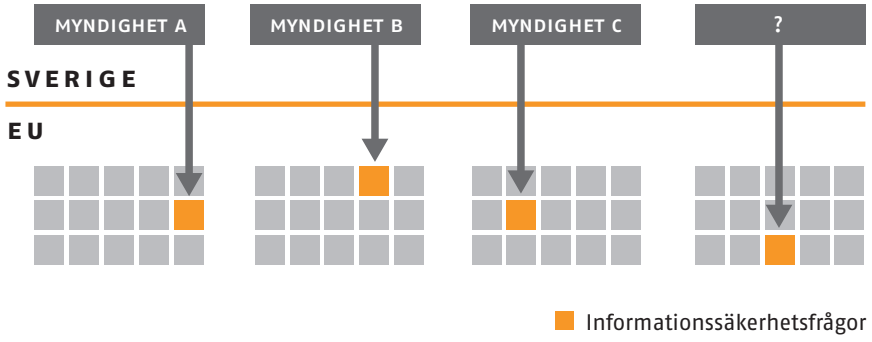
Genomförandefas

Efter det att inriktningsfasen avslutats tog genomförandefasen vid. Inledningsvis fördjupades den litteraturinventering som påbörjats under den första fasen, förutom litteratur i form av böcker, rapporter och PM söktes även material via nätet. En given källa till information har varit de offentliga EU-arkiven.

De personer som intervjuades under inriktningsfasen påtalade svårigheten med att läsa sig till en förståelse för området och poängterade vikten av att så snart som möjligt genomföra intervjuer med relevanta aktörer. Projektet anammade denna strategi och genomförde två omfattande intervjuserier – en nationell, med huvudsakligt fokus på myndighetsaktörer, och en europeisk där vi intervjuade personer hemmahörande i relevanta organisationer och forum.

Några ord om intervjuserierna. De intervjuer som genomfördes under inriktningsfasen visade att det kunde vara svårt att hitta rätt i EU-maskineriet, inte minst när det gäller ingångar för intervjuer. Därför valde vi att börja med att kartlägga ett urval av de svenska myndigheternas kontaktytor (och givetvis dess innehåll)[9] med aktörer på EU-nivån, se illustrationen nedan:

Genom att börja lägga ”pusslet” på nationell nivå var förhoppningen att dels skapa en förståelse för det arbete och de kontakter som redan finns i dag, och dels att underlätta kontaktskapandet på EU-nivån. I vissa fall visade sig denna arbetshypotes stämma, men i ganska stor utsträckning fanns det relativt begränsade kontaktytor mellan de svenska myndigheterna och de europeiska institutionerna och organen. Detta resulterade i att projektgruppen snart fick övergå till två parallella spår där



Figur 2. *Kartläggningsprocess.*

9. Att skapa en överblick över de svenska erfarenheterna på EU-nivå ligger även i linje med det policy- och samordningsansvar som InfoSäkutredningen föreslår KBM i sitt slutbetänkande. Detta uttrycks bl.a. som: ”En uppgift bör också vara att säkerställa att alla myndigheters internationella erfarenheter inom området informationssäkerhet tas till vara”. Se InfoSäkutredningens slutbetänkande SOU 2005:71, sid. 89.

resultaten från de nationella intervjuerna (när det gäller faktiska kontakter) fick kompletteras med sökningar via nätet samt en initial intervjurunda i Bryssel för att skapa fler kontakter.

Eftersom intervjuserierna utgjort det viktigaste redskapet för informationsinhämtning har projektgruppen lagt stor vikt vid att dokumentera dessa på ett lämpligt sätt. I vissa fall – främst när det gäller de svenska myndigheterna – har de intervjuade personerna även fått möjlighet att komplettera anteckningarna.

Analysfas

I analysfasen bearbetades det insamlade materialet och de initiala frågeställningarna besvarades utifrån det material och de insikter som gjorts. Projektgruppen arbetade intensivt tillsammans under analysfasen, bl.a. genomfördes ett antal interna seminarier i syfte att skapa insikter och lärdomar ur det insamlade underlaget. Vidare använde sig projektgruppen av en programvara, MindManager®, för att skapa ett grafiskt ramverk för själva kartläggningen.

Kommunicerandefas

I denna fas producerades denna rapport samt den kartläggning i form av en Mindmap-struktur som är att se som slutleveranser för studien. Dessa är tänkta att användas tillsammans som ett verktyg för dem som är intresserade av att öka sina kunskaper om den informationssäkerhetsrelaterade verksamhet som bedrivs inom EU.

Metodologiska överväganden och avgränsningar

Nedan presenteras några aspekter som påverkat vilka metoder som har använts i studien. Här redovisas även de ansatser som gjorts för att minimera dessa aspekters potentiellt negativa inverkningar på studiens genomförande och resultat.

Vad är informationssäkerhet? Sakfrågan som styr studien

Hur studerar man ett problemområde med ”rörligt” innehåll? Informationssäkerhet är ett mångfacetterat begrepp som dessutom innebär olika saker för olika aktörer. Som forskare gäller det att inte enbart förhålla sig till det faktum att olika aktörer använder sig av olika begrepp – fastän de ibland menar samma sak – utan även till att de ibland använder sig av samma begrepp fastän de fyller det med olika innehåll (en insikt som är värdefull även för andra aktörer).

En annan svårighet är att inte bara det som specifikt rubriceras som informationssäkerhet är relevant i sammanhanget. Ofta hanteras inte informationssäkerhetsfrågor explicit och fristående inom EU-arbetet, utan ingår som delfrågor i andra frågekomplex.

Mot bakgrund av den ovanstående problembilden har projektgruppen använt sig av en ansats som består av två huvudsakliga delmoment vid genomförandet av intervjuerna:

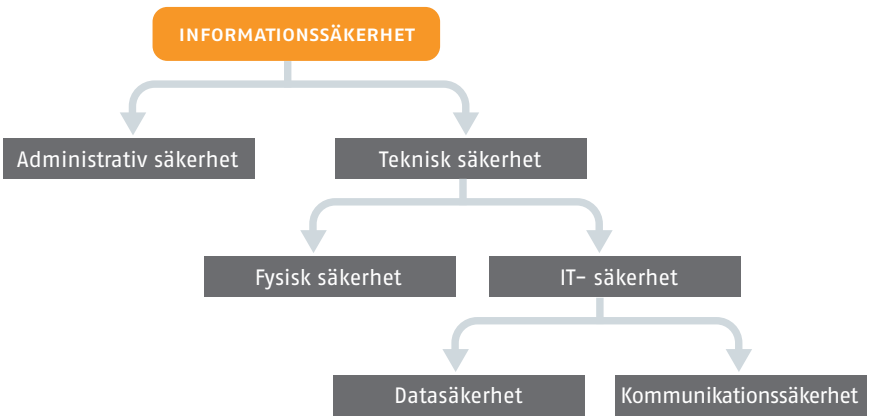
Klargörande av begrepp

Hur definierar intervjupersonerna informationssäkerhetsbegreppet? Vilken betydelse lägger de tillfrågade personerna i begreppet? Det är viktigt att klargöra deras syn på begreppets innebörd för att i sin tur kunna värdera deras svar. Projektgruppen har vid intervjutillfällena presenterat olika alternativ till hur informationssäkerhet kan definieras – se två exempel nedan – för att skapa underlag för en diskussion kring de intervjuades respektive syn på frågeområdet.

Ett möjligt sätt att definiera informationssäkerhet är utifrån följande begrepp:

- Konfidentialitet – *Försäkran om att information inte avslöjas till någon obehörig.*
- Autentisering – *Validering av identitet eller annan unik egenskap hos en individ eller enhet.*
- Auktorisering – *Försäkran om att endast behöriga personer eller enheter har åtkomst till något.*
- Integritet och riktighet – *Skydd mot otillbörlig förändring av information efter det att den lämnat avsändaren.*
- Oavvislighet – *Förhindra att någon part i efterhand kan förneka sin delaktighet i en transaktion.*
- Tillgänglighet – *Försäkran om att en tjänst inte blir otillgänglig.*
- Spårbarhet – *Händelser loggas så att de kan spåras och återskapas vid behov.*

Ett annat sätt är att utgå från en mer schematisk indelning:[10]



Figur 3. *Informationssäkerhet enligt SIS.*

10. Illustrationen återfinns i SIS tekniska rapport Handbok 550: Terminologi för informationssäkerhet (2003). Den finns även i InfoSäkutredningens Delrapport 2 ”Informationssäkerhet i Sverige och internationellt – en översikt”, SOU 2004:32.

Identifiering av relevanta verksamheter kopplade till politikområden

Förutom att tydliggöra intervjupersonernas syn på innebörden av begreppet informationssäkerhet har projektgruppen även valt att utifrån de centrala begreppen (se ovan) definiera möjliga politikområden[11] och relaterade verksamheter som sedan använts vid intervjuerna i exemplifierande syfte. Detta för att, om möjligt, få intervjupersonerna att förhålla sig till frågor som de kanske inte först skulle valt att adressera. Det bör påpekas att vi inte alltid varit helt konsekventa i att använda denna metodansats utan den har snarast tillämpats i de fall det ansetts fruktbart.

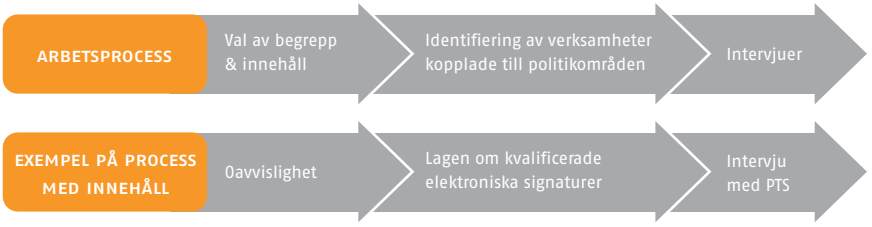
Nedan följer en illustration där detta tillvägagångssätt exemplifieras av begreppet oavvislighet.

Urval och avgränsningar av studieobjekt

I den inriktningspromemoria som författades i december 2005 listades ett antal potentiella studieobjekt att utgå ifrån i det kommande arbetet.[12] Med dessa som utgångspunkt genomfördes en genomgång av vilka avgränsningar som kunde vara lämpliga för studien och intervjuserierna. Nedan följer en kort genomgång av de avgränsningar som slutligen styrt de studieobjekt som ingått i studien.

Nationell intervjuserie – myndigheter i blickfånget

På nationell nivå utgick studien främst från myndighetsrelaterade aktörer och deras kontaktytor med EU. Denna avgränsning mynnar ur formuleringen av det samordningsansvar som KBM har inom informationssäkerhetsområdet.



Figur 4. *Exemplifierande arbetsprocess.*

11. Ett politikområde definierar ett tematiskt område för vilket det bedrivs specifik politik. Det kan vara exempelvis miljöområdet, handelsområdet, försvarsområdet etc.
12. Se not nr. 8.

Bi- och multilateralt arbete mellan EU:s medlemmar och mellan EU:s aktörer, medan EU-externa parter exkluderas

När det gäller informationssäkerhetsrelaterad verksamhet som bedrivs inom EU har vi valt att bara fokusera på verksamhet och aktörer som befinner sig inom EU:s institutionella ramar. Vi har alltså valt bort bi- och multilaterala (där EU-externa parter deltar) initiativ. Denna avgränsning har gjorts på både grundval av studiens inriktning och dess tids- och budgetmässiga ramar.

På EU-nivån: fokus där möjlighet till påverkan finns (EU-kommissionen)

Ett av syftena med studien var att skapa förutsättningar för svenskt agerande och tillvaratagandet av svenska intressen i EU-sammanhang. Därför har studien i stor utsträckning kommit att fokusera kring EU-kommissionens verksamhet, eftersom den har en given roll i bl.a. initiativfasen.[13]

I initiativfasen behandlas sakfrågorna och underlag tas fram för att kunna utgöra grund för den fortsatta behandlingen inom EU. Myndighetsaktörer på nationell nivå kan sägas ha störst möjlighet att påverka vilka frågor som tas upp och hur dessa ska prioriteras och formuleras i denna fas. Vikten av att agera redan under initiativfasen är något som betonats i flera sammanhang, bl.a. har UD tagit fram ett cirkulär där vikten av ett aktivt svenskt agerande i just initiativfasen framhålls.[14]

Att EU-kommissionen hamnat i fokus betyder dock inte att andra aktörer på EU-nivån avgränsats bort, utan bara att tyngdpunkten i vårt arbete – inte minst intervjuerna – kommit att hamna på EU- kommissionens arbete.

EU:s interna informationssäkerhetsarbete exkluderas i studien

Inom EU pågår givetvis ett arbete med att stärka den egna informationssäkerheten. I detta arbete är exempelvis aktörer som generalsekretariatets säkerhetsavdelning (inom Europeiska rådet) en viktig faktor. När det gäller denna studie har vi valt att inte närmare fördjupa oss i det interna säkerhetsarbetet och de interna strukturerna som finns för att hantera informationssäkerhetsproblematiken. Detta har inte ansetts ligga inom ramen för studiens huvudsakliga fokus, lika lite som svenska myndigheters interna säkerhetsarbete ansetts vara relevant. Detta är dock ett område som det finns anledning att återkomma till i framtida studier eftersom EU:s interna informationssäkerhetsarbete i förlängningen kan komma att påverka svenska myndigheters interna informationssäkerhetsarbete.

13. För mer om EU-kommissionens roll se avsnitt *Vilka är EU:s centrala aktörer.*
14. Se ”Cirkulär med riktlinjer för handläggningen av kommissionens offentliga samråd”, Utrikesdepartementet, 2004-06-08.

Frågor med utpräglad militär prägel (Cyber Defence) avgränsas bort

För detta projekt har vi valt bort frågor av utpräglad militär karaktär, även de som är kopplade till forskning, materielfrågor, militära operativa koncept m.m. I stället har arbetet fokuserats kring frågekomplex som inom EU faller under rubrikerna ”Cyber Security”, ”Cyber Crime” och i viss mån ”CIIP” (Critical Information Infrastructure Protection).

Genomförda intervjuer i Sverige och EU

Sammantaget genomfördes 35 stycken intervjuer i Sverige och EU (Bryssel) omfattande totalt 46 personer. Intervjuerna har varit semistrukturerade och explorativa till sin karaktär. För varje intervju har en separat intervjuguide tagits fram. Genomgående har stor frihet byggts in i formatet för att säkerställa möjligheten att följa intervjupersonens resonemang dit de bär. Ambitionen har inte varit att genomföra en komparativ studie och därför har den begränsade möjligheten till jämförelser inte inneburit något problem.

Genomgående får responsen vid förfrågan om att genomföra intervjuer sägas ha varit god, även om det tagit relativt mycket arbete i anspråk att ”få till” rätt intervjuer. I de fall våra svenska myndighetsrepresentanter har tillhandahållit kontakter på EU-nivå har processen att boka in intervjuer gått smidigt och enkelt. I de fall ett befintligt kontaktnät saknas har det varit svårare att nå fram. Detta belyser vikten av att upprätthålla goda kontaktnät och att kunna samordna olika aktörers kontaktnät för att uppnå synergieffekter.

Nedan följer en svensk och en ”EU-inriktad” tabell där de organisationer vi intervjuat finns listade.[15]

SVENSKA AKTÖRER		
DEPARTEMENT	**MYNDIGHETER**	**IDEELL FÖRENING**
Näringsdepartementet	FHS	SIS
Justitiedepartementet	FOI	
Försvarsdepartementet	FMV	
Utrikesdepartementet (EU-representationen i Bryssel)	FRA	
	PTS	
	Riksbanken	
	Rikskriminalpolisen	
	SWEDAC	
	VERVA	
	Datainspektionen	

Tabell 1. *Svenska aktörer som intervjuats.*

15. Här inkluderas intervjuer på plats, via telefon eller per e-post.

EU-AKTÖRER		
EU-KOMMISSIONEN	**RÅDET**	**PARLAMENTET**
DG JFS (Generaldirektoratet för rättvisa, frihet och säkerhet) Enhet D/1: Fight against terrorism, trafficking and exploitation of human beings and law enforcement Enhet D/2: Fight against economic, financial & cyber crime Enhet D/5: Data Protection	**Arbetsgrupper:** Sektorsöverskridande arbetsgruppen mot organiserad brottslighet Arbetsgruppen för forskning Arbetsgruppen för telekommunikationer och informationssamhället	Utskottet för inre marknaden och konsumentskydd Utskottet för medborgerliga fri- och rättigheter
DG InfSo (Generaldirektoratet för informationssamhälle och medier) Enhet H/4: eTen Enhet D/4: ICT for trust and security Enhet A/3: Internet, network and information security	**Rådssekretariatet:** DG H – Justice and Home Affairs DG C – Internal market, competitiveness, industry, research, energy, transport, information society	
DG TREN (Generaldirektoratet för energi och transport) Enhet B/2: Policy for energi and transport Enhet B/5: Satellite navigation system (Galileo), intelligent transport		
DG Enterprise & Industry (Generaldirektoratet för näringsliv och industri) Enhet H/4: PASR Enhet I/5: European eGovernment Services		

MYNDIGHETER	STANDARDISERINGSAKTÖRER	DECENTRALISERADE ORGAN
Enisa	CEN[16] (European Committee for Standardisation)	Europol ISS (European Institute for Security Studies)[17]

Tabell 2. *EU-relaterade aktörer som intervjuats.*

16. Genom dess vice president eller ordförande (tekniska delen) Lars Flink som även är VD för SIS. Se mer under avsnitt *Övriga aktörer*.
17. Kontakten med ISS bestod mer av kontaktförmedling än en genomgång av deras verksamhet.

Mycket är gjort – mycket återstår

Informationssäkerhet är en fråga som rör all typ av verksamhet som bedrivs inom EU. Det finns inte många politikområden där det inte går att hitta informationssäkerhetsrelaterade frågeställningar. Även här i Sverige återfinns olika aspekter av problematiken inom olika politikområden och såväl hanterings- som ansvarsmässigt faller frågorna på olika departement, myndigheter och privata aktörer inom alla samhällssektorer. Naturligtvis får detta konsekvenser för denna typ av kartläggningsstudie – det finns alltid fler aktörer att kartlägga! Vi i projektgruppen anser dock att vi identifierat de mest relevanta aktörerna utifrån våra avgränsningar.

En viktig avvägningsfråga i en kartläggningsstudie är vilken detaljnivå som ska eftersträvas. Vår avsikt har huvudsakligen varit att spänna upp området och tillhandahålla hänvisningar till vidare information. Inom vissa områden där vi har kunnat göra intervjuer eller där det funnits lättillgänglig information har vi nått en högre detaljnivå än inom andra områden.

Detta sagt vill vi poängtera att *resultaten från denna studie ska ses som ett första försök att kartlägga de relevanta aktörerna inom EU*. Förhoppningen är att arbetet kan fortsätta vid KBM så att bilden hålls uppdaterad och undan för undan kan kompletteras och fördjupas.

Övrigt underlag

Frågan om material har i korthet berörts tidigare i rapporten. Nedan återfinns en något mer strukturerad genomgång över det material som studien baseras på. Till övervägande del bygger studien på de intervjuserier som genomförts på nationell och europeisk nivå, men dessa har även kompletterats med litteraturstudier. Materialet har i huvudsak sökts inom följande kategorier:

- Facklitteratur på området, exempelvis rapporter.
- Författningar och regleringsbrev.
- Direktiv m.m., EU:s offentliga arkiv (åtkomligt via Internet).
- Information kopplad till de europeiska organisationernas respektive verksamhet, åtkomlig i huvudsak via Internet.

Hänvisningar till detta material återfinns kontinuerligt i rapporten där det anses relevant.

Projektgrupp

Projektgruppen har bestått av följande personer:

- Malin Fylkner, FOI (PL)
- Svante Barck-Holst, FOI
- Helén Jarlsvik, FOI, EU expertresurs
- Linda Englund, KBM, (fr.o.m. januari 2006.)

Projektet har bemannats utifrån de olika kompetenskrav och behov som följer av studiens syfte.

Introduktion till EU

Detta kapitel är skrivet för de personer som är behjälpta av en kort introducerande text till EU. I kapitlet finns en översiktlig beskrivning av EU tillsammans med svar på frågor som: Inom vilka områden bedriver EU politik? Vilka är EU:s institutioner? Hur ser EU:s beslutsprocesser ut? Vad blir resultatet av EU:s politik? Hur involveras svenska myndigheter i EU:s arbete?

Inom vilka områden bedriver EU politik?

I det europeiska integrationsprojektets begynnelse var samarbetet främst inriktat på ekonomiska frågor. I dag verkar EU dock inom de flesta politikområden som står på den politiska dagordningen i en enskild stat. Jordbruksfrågor, transportfrågor, miljöfrågor, konsumentfrågor, utrikespolitiska frågor samt rättsliga och polisiära frågor är några exempel på områden där unionen i olika utsträckning stiftar lagar, förvaltar program, utarbetar gemensamma ståndpunkter, organiserar evenemang m.m.

Vilka områden som EU ska ägna sig åt och med vilken ambitionsnivå bestäms i EU:s fördrag. För att EU ska kunna bedriva politik inom ett visst område måste det finnas tydligt lagligt stöd ”legal grund” i fördragen. Ofta kan ett visst politikområde hänföras till en eller flera specifika artiklar i fördragen som behandlar det aktuella området. Ibland används dock en ”restkompetensparagraf”, artikel 308, som något förenklat går ut på att EU ges rätt att verka inom ett visst område, utan att detta nämns explicit i fördragen, om politiken bidrar till att målen med den europeiska gemenskapen uppfylls.

De områden som EU bedriver politik inom brukar delas in i tre s.k. pelare: den europeiska gemenskapen (första pelaren), den gemensamma utrikes- och säkerhetspolitiken (andra pelaren) samt det inrikes- och rättsliga samarbetet (tredje pelaren). Pelarindelningen är ett sätt att markera att medlemsstaternas grad av inflytande, och sättet på vilket beslut fattas, skiljer sig åt något mellan olika politikområden. Den första pelaren, där de flesta politikområden ingår, är exempelvis mer

överstatlig till sin karaktär än arbetet i den andra och tredje pelaren som i stället präglas av mellanstatlighet.

För närvarande gäller de s.k. EG- och EU-fördragen. Ett nytt samlat konstitutionellt fördrag har dock förhandlas fram av Europas stats- och regeringschefer. Eftersom det nya fördraget inte har ratificerats av alla medlemsstater ännu kommer det dock sannolikt att dröja flera år innan fördraget träder i kraft, och då troligen i modifierad form. Det nya konstitutionella fördraget innehåller en rad nyheter. En viktig förändring som förutses är att de politikområden som för närvarande ingår i den tredje pelaren kommer att hanteras på samma sätt som politikområdena i den första pelaren. Endast den gemensamma utrikes- och säkerhetspolitiken skulle i så fall ha kvar en särställning. Därmed skulle pelarindelningen i praktiken upphöra.

Vilka är EU:s centrala aktörer?

EU:s fördrag lägger inte bara fast inom vilka områden som EU ska bedriva politik, utan fördragen tydliggör också vilka EU:s institutioner är och vilken roll dessa institutioner har i arbetet med att formulera och genomföra EU:s politik.

Europeiska kommissionen bevakar det överstatliga gemensamma intresset i EU-samarbetet och tar initiativ till och utarbetar förslag till nya rättsakter för unionen. I den första pelaren har kommissionen en särskilt stark roll som ensam initiativtagare till politiken. I första pelaren är kommissionen också verkställande organ och ansvarar därmed för att de beslut som fattas av rådet och parlamentet genomförs. Avslutningsvis övervakar kommissionen att EU:s fördrag och beslut följs. Om kommissionen anser att en medlemsstat bryter mot de ingångna överenskommelserna har kommissionen möjlighet att ställa densamme inför rätta i EG-domstolen.

Kommissionen består av ett tjugotal kommissionärer som stöds av olika generaldirektorat (GD) med egna ansvarsområden samt ett antal stabsfunktioner och andra enheter. Generaldirektoraten är tematiskt indelade och därför finns det ett GD för transportfrågor, ett för miljöfrågor, ett för jordbruksfrågor osv.

Ministerrådet för de enskilda medlemsstaternas talan i EU-samarbetet och är unionens högsta beslutande organ. Rådet granskar och beslutar om kommissionens förslag till rättsakter, initierar egna förslag inom den andra respektive tredje pelaren, bestämmer tillsammans med parlamentet EU:s budget samt sluter internationella avtal mellan EU och andra stater och organisationer.

Arbetet i rådet bedrivs på tre nivåer, på tjänstemannanivå i olika tematiskt indelade rådsarbetsgrupper, på hög tjänstemannanivå i de ständiga representanternas kommitté (Coreper) som består av medlemsstaternas EU-ambassadörer, och i själva ministerrådet där medlemsstaternas fackministrar träffas. Ministerrådet kan mötas i olika forma-

tioner beroende på frågans karaktär. Rådets arbete leds av ett ordförandeland som har stor möjlighet att påverka EU:s dagordning. Ordförandeskapet växlar varje halvår. För kontinuiteten i rådsarbetet svarar det s.k. rådssekretariatet som utgör rådets stabsfunktion och som stöttar ordförandeskapet i förhandlingsarbetet.

Europaparlamentets huvuduppgift i EU-samarbetet är att fatta beslut och att utöva demokratisk kontroll. Konkret innebär det bland annat att inom vissa politikområden i den första pelaren, tillsammans med rådet granska och bestämma om kommissionens initiativ till rättsakter kan antas samt att godkänna EU:s budget och kommissionens sammansättning. Parlamentet har ingen beslutfattande roll i den andra och tredje pelaren men ska vanligtvis hållas informerad om de beslut som fattas.

EG-domstolen är EU:s domstol som tolkar det gemensamma regelverket och dömer i tvister om tillämpningen av EG-rätten. Domstolen kan döma i tvister mellan medlemsstaterna, mellan EU:s institutioner och medlemsstaterna, mellan institutionerna samt mellan EU:s institutioner och företag eller enskilda personer. EG-domstolen består av 15 domare som biträds av 8 generaladvokater och utses av medlemsstaterna.

Andra centrala aktörer i EU-samarbetet är de *EU-myndigheter*[18] som har inrättas som kompetenscentrum inom olika områden. Dessa är vanligtvis organisatoriskt nära knutna till kommissionen. Ett exempel på en sådan myndighet är ECDC, det europeiska centrumet för förebyggande och kontroll av sjukdomar, som bl.a. har till uppgift att bidra till att stärka Europas försvar mot infektionssjukdomar som influensa, SARS samt hiv och aids.[19]

Mycket viktigt är också *Europeiska rådet*, som formellt sett inte är en fördragsfäst EU-institution, men som ändå har ett stort inflytande över EU:s politik. Europeiska rådet är stats- och regeringschefernas särskilda forum. Vid Europeiska rådets möten, som vanligen sker ett par gånger om året, medverkar även kommissionens ordförande. Europeiska rådet har en viktig roll som politisk visionär för EU-samarbetets övergripande framtida inriktning och är det organ som förhandlar fram EU:s fördrag.

Hur ser EU:s politiska beslutsprocess ut?

Processen där EU-politiken formas varierar något mellan de tre pelarna, framförallt beroende på att institutionerna har olika grad av inflytande i dessa pelare. Något förenklat kan beslutsprocessen delas in i en initiativfas, en beslutfas och en genomförandefas.

18. Ibland kallas också myndigheterna för gemenskapsbyråer.
19. http://europa.eu/agencies/community_agencies/ecdc/index_sv.htm 2006-06-21.

Initiativfasen kan vara relativt lång, särskilt i den första pelaren, och består av alla de aktiviteter som bidrar till att ny lagstiftning eller ny politik formuleras. För att få underlag till exempelvis lagstiftningsarbetet, och för att öka dess legitimitet, anordnar kommissionen och ibland rådet olika typer av öppna seminarier, konferenser eller konsultationer (via Internet i det senare fallet) där myndigheter, intresseorganisationer och andra grupperingar kan delta. Ibland anordnar också kommissionen mer begränsade expertmöten. Experterna från medlemsstaternas myndigheter eller andra organisationer deltar då vanligtvis i sin personliga kapacitet.

I *beslutfasen* spelar rådet en helt central roll. Det är där som medlemsstaternas intressen bevakas. Förhandlingarna mellan de tjugofem medlemsstaterna inleds alltid i rådsarbetsgrupper på tjänstemannanivå. Dessa bemannas vanligtvis med delegater från medlemsstaternas Brysselbaserade EU-representationer, men ibland sköts förhandlingarna av ditresta departementstjänstemän från medlemsstaternas huvudstäder. Eventuella utestående frågor omhändertas av Coreper och därefter av själva ministerrådet. Ofta handlar ministerrådets arbete bara om att formellt godkänna en redan färdigförhandlad text. Om omröstning krävs varierar omröstningsförfarandet beroende på vilket politikområde det är frågan om. I den andra och tredje pelaren är det enhällighet som gäller. I den första pelaren är det däremot vanligt med kvalificerade majoritetsbeslut. Medlemsstaterna har dessutom olika antal röster beroende på landets storlek. I politikområden i den första pelaren där parlamentet har beslutsrätt ska även parlamentet godkänna de rättsakter som kommissionen föreslår. Ett beslutsförfarande där parlamentet involveras tar ofta relativt lång tid och ibland måste förslaget tas till en förlikningskommitté där kommissionen, parlamentet och rådet tillsammans försöker hitta en lösning.

Genomförandefasen är den längsta och mest mångskiftande av de tre faserna. Det handlar bl.a. om att, i den första pelaren, precisera den övergripande lagstiftning och politik som har förhandlats fram i beslutfasen genom att ta fram mer konkreta regler, arbetsprogram eller kanske dela ut pengar till olika projekt. I detta arbete spelar kommissionen en central roll. Kommissionens ansvar för genomförandet begränsas dock genom s.k. genomförandekommittéer. När en rättsakt antas skrivs man ofta in skapandet av en genomförandekommitté, eller utnyttjandet av en befintlig kommitté. I dessa kommittéer hålls förhandlingar om olika detaljerade beslut (jfr diskussionen om regler, arbetsprogram och projekt ovan) och kommissionen sitter ordförande. Alla medlemsstater är dock också representerade. Genomförandefasen handlar också om att aktivt utföra eller inhämta resultatet av EU:s politik. Det kan röra sig om allt från att anpassa svensk lagstiftning till EU:s direktiv till att delta i forskning eller anordna utbildningar som finansieras av EU.

Vad blir resultatet av EU:s politik?

Processen där EU:s politik formas resulterar i en mängd olika typer av dokument. I initiativfasen är dokument från kommissionen vanligt förekommande, åtminstone om dokumentet berör ett politikområde i den första pelaren. Grönböcker innehåller relativt övergripande idéer och tankar från kommissionens sida om möjliga åtgärder inom ett visst område. En grönbok är ofta det första dokumentet i beslutsprocessen och inleder vanligtvis en konsultationsrunda där berörda aktörer i medlemsstaterna får komma med synpunkter på kommissionens idéer. Ibland följs en grönbok av lanseringen av en vitbok där kommissionen ofta är mer specifik i sina förslag till åtgärder. Meddelanden (”communications”) från kommissionen till rådet och parlamentet är också mycket vanligt förekommande i initiativfasen. De liknar grön- och vitböckerna, men är ofta mer offensiva och tydliggör vilka åtgärder, exempelvis kommande lagförslag, som kommissionen tänker vidta inom ett visst område. Ofta resulterar meddelandena i att medlemsstaterna antar s.k. rådsslutsatser i rådet där kommissionens planer kommenteras.

När kommissionen presenterar ett dokument som innehåller ett förslag till rättsakt (”proposal for a…”) markerar detta en övergång från initiativfasen till beslutfasen. Dokumentet kommer då att bli föremål för förhandlingar i en rådsarbetsgrupp, och i vissa fall i parlamentet. Det finns flera olika typer av rättsakter, både bindande och icke-bindande, och dessa varierar något mellan de tre pelarna. I den första pelaren är förordningar, direktiv, beslut samt rekommendationer och yttranden vanliga. En förordning som har trätt i kraft gäller direkt och på samma sätt i alla medlemsstater. Medlemsstaterna behöver inte vidta några åtgärder för att förändra sina nationella lagar. Samtidigt står förordningen över medlemsstaternas nationella lagar. Ett direktiv föreskriver vilka mål som medlemsstaterna ska uppnå och när, men medlemsstaterna får själva avgöra på vilket sätt. Handlingsutrymmet för de enskilda staterna är alltså något större. Ett beslut kan användas för många olika typer av ändamål och gäller direkt för den eller de medlemsstater, fysiska eller juridiska personer som beslutet riktar sig till. Rekommendationer och yttranden, slutligen, är två typer av icke-bindande rättsakter som innebär att medlemsstaterna inte är skyldiga att följa dem. Överenskomna dokument publiceras alltid i EU:s Official Journal of the European Union.

Ibland är överenskomna rättsakter alltför övergripande till sin karaktär och i genomförandefasen måste därför detaljerna i beslutet preciseras av kommissionen, med stöd av olika typer av genomförandekommittéer. Resultatet av detta arbete presenteras i s.k. kommissionsbeslut. De rättsakter som innebär att pengar ska fördelas till projekt preciseras vanligtvis i en arbetsplan

(”workplan”) som tas fram i form av ett kommissionsbeslut.

Det konkreta innehållet i den relativt breda uppsättning av dokument som varje dag produceras i EU:s beslutsprocess är lika mångskiftande som antalet politikområden på EU:s agenda. Därför ges enbart några få exempel här inom krisberedskapsområdet. Inom detta område är det yttersta syftet med EU:s politik att stärka säkerheten i Europa genom att reducera sårbarheter eller stärka förmågan att hantera kriser. I de dokument som förhandlas fram kan EU bl.a. bidra till detta genom att ställa olika typer av *krav* på hur medlemsstaterna ska sköta sin nationella beredskap (krav på medlemsstaternas livsmedelshantering, gränskontrollssystem, säkerhetsarrangemang i hamnar osv.). EU kan också bidra till att stärka säkerheten i Europa genom att knyta *ekonomiska medel* till de dokument som förhandlas fram och dela ut pengar till olika typer av krisberedskapsprojekt i medlemsstaterna (studier, forskning, övningar, utbildningar osv.). Slutligen kan EU bidra till att stärka säkerheten i Europa genom att förmedla *information* och *insatsresurser* i en akut krissituation, via olika informations- och resursförmedlingsarrangemang som inrättas genom de dokument som förhandlas fram.

Hur berörs svenska myndigheter av EU:s politik?

I dag är EU-arbetet en integrerad del i Sveriges politik, oavsett om det rör sig om inrikes- eller utrikespolitiska frågor. Sverige påverkas av EU:s politik och måste därför också aktivt påverka densamma. För svenska myndigheter handlar det i dag om att vara aktiva i både initiativ- och genomförandefasen.

I initiativfasen är det svenska myndigheter som vanligtvis representerar Sverige vid seminarier, på konferenser och vid andra möten. Efter den senaste utvidgningen består EU av 25 medlemsstater vilket har gjort det svårare att få gehör för svenska ståndpunkter i beslutfasens förhandlingsarbete. Därför har det blivit allt viktigare att aktivt påverka politikens inriktning i initiativfasen, redan innan konkreta förslag läggs. Myndighetsexperter representerar Sverige och svenska intressen i denna fas och det är därför viktigt att de ståndpunkter som framförs har stämts av med Regeringskansliet.[20]

I beslutsfasen spelar svenska myndigheter vanligtvis en något mindre framträdande roll än i initiativfasen och genomförandefasen. Ofta deltar myndighetsrepresentanter som expert-

20. UD har tagit fram ett cirkulär där vikten av ett aktivt svenskt agerande i initiativfasen framhålls, liksom behovet av nära dialog mellan myndighetsexperter och Regeringskansliet. Se tidigare hänvisning, not nr 17, för mer information.

stöd till sitt respektive departement när instruktioner till rådets möten skrivs. Ibland kan de också bisitta den svenska representanten (från EU-representationen eller Regeringskansliet) i de rådsarbetsgrupper där merparten av rådets förhandlingsarbete bedrivs.

I genomförandefasen spelar svenska myndigheter återigen en central roll. Vanligtvis, men inte alltid, är det myndighetsrepresentanter som deltar i kommissionens genomförandekommittéer för Sveriges räkning. Det är ofta myndigheter som hämtar hem resultatet av EU:s politik genom att utföra de projekt som EU finansierar, skapa nationella arrangemang som länkar upp mot olika informations- och resursförmedlingssystem etc. Myndigheter berörs också i sitt dagliga tillsynsarbete när svensk lagstiftning anpassas till EU:s rättsakter.

Informationssäkerhet i Sverige och EU – begrepp i fokus

Olika aktörer använder olika definitioner av centrala begrepp, vilket försvårar interaktion över såväl organisatoriska som geografiska gränser. Ett viktigt steg i att minimera konsekvenserna av språkförbistring (och därmed öka förutsättningarna att nå större framgång i exempelvis kontakterna med EU:s företrädare) är att vara medveten om de skillnader och likheter som finns bland begreppen. Mot bakgrund av detta presenteras nedan några centrala definitioner och perspektiv på begreppet informationssäkerhet. Kapitlet är av bakgrundskaraktär.

Nät- och informationssäkerhet enligt EU:s definitioner

Den ”EU-definition” som ofta förs fram i offentliga texter och presentationsmaterial är den som presenteras i kommissionens förslag till en europeisk strategi. Där finns denna definition av informationssäkerhet:

”The ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services that may be offered by these networks and systems”.[21]

Översatt till svenska blir detta:

“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”.[22]

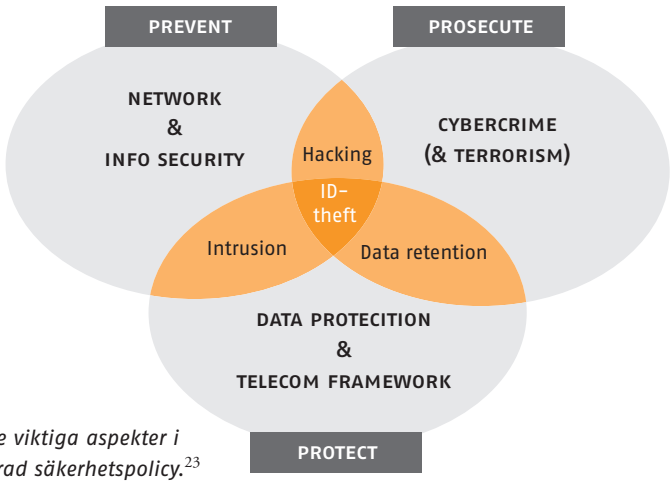
Intressant i detta sammanhang är att notera att flera av de begrepp som presenterades tidigare under avsnitt Vad är informationssäkerhet? Sakfrågan som styr studien (som tillgänglighet och

21. Definitionen återfinns bl.a. i kommissionens ”Nät och informationsstrategi – Förslag till en europeisk strategi”, KOM/2001/0298.
22. Ibid.

konfidentialitet) återfinns även i EU-definitionen, men att det även finns viktiga skillnader. Exempelvis återfinns **inte** begrepp som *spårbarhet* och *oavvislighet* vilka – sett ur ett svenskt perspektiv – är två viktiga aspekter i definierandet av informationssäkerhetsbegreppet.

Hur förhåller sig då begreppet informationssäkerhet till andra centrala begrepp (exempelvis cyberbrottslighet, data protection m.m.) inom EU? Ett sätt att besvara denna fråga är att utgå från den modell som ofta används i olika EU-sammanhang där begreppen kopplas till de olika handlingsstrategierna: förebygga (prevent), skydda (protect) och beivra (prosecute). Se nedan. Som framgår av illustrationen finns det inga vattentäta skott mellan de olika dimensionerna och begreppen, utan de överlappar varandra. Detta är karaktäristiskt för problemområdet och något som komplicerar hanterandet av relaterade frågor. Eftersom ansvarsfrågan inom EU till stor del styrs av inom vilka pelare som frågorna hamnar, medför överlappningarna att en och samma fråga – eller åtminstone olika aspekter av samma fråga – kan hanteras av olika aktörer inom EU.

Inom kommissionen hanteras frågor kring nät- och informationssäkerhet (omnämns ofta som Cyber Security) inom generaldirektoratet för informationssamhälle och medier (DG InfSo), medan frågor kopplat till cyberkriminalitet och skydd av personuppgifter (data protection) faller under generaldirektoratet för rättvisa, frihet och säkerhet (DG JFS). Frågor kopplade till cyberterrorism återfinns på flera aktörers bord, bl.a. DG JFS.



Figur 5. *Tre viktiga aspekter i en integrerad säkerhetspolicy.*[23]

23. Ibid. Det cirkulerar lite olika versioner av denna bild. De begrepp som är satta inom parentes ingår inte i den version som presenteras i strategin. I denna rapport ingår även de begreppen i diskussionstexten.

När det gäller skydd av kritisk infrastruktur (CIP), eller mer exakt skydd av kritisk informationsinfrastruktur (CIIP), har DG JFS tagit en ledande roll (särskilt för de policymässiga aspekterna). CIP och CIIP hanteras i huvudsak som en helhet inom EU eftersom det är svårt att avgränsa de respektive frågeområdena.[24]

Svensk begreppssyn

Det finns ingen nationell definition av begreppet informationssäkerhet. Däremot kan den definition som InfoSäkutredningen valt att utgå från (vilket i grunden är en vedertagen SIS-definition) antas ha fått stor spridning. I den versionen får informationssäkerhet följande definition:

”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”.[25]

Utgångspunkten för denna definition är att information x för aktör y är kritisk och att om den ändras, förstörs eller görs otillgänglig äventyras aktören y:s verksamhet (eller en resurs som är viktig för denna aktör). På samma sätt kan aktörens verksamhet äventyras om verksamheten inte vidtagit tillräckliga åtgärder för att skydda informationen. Av detta framgår att både IT-säkerhet och administrativ säkerhet utgör viktiga komponenter i begreppet informationssäkerhet.[26]

Skillnaden mellan teori och praktik – vilka begrepp gäller?

Erfarenheter från de genomförda intervjuserierna visar att det kan finnas avsevärda svårigheter med att använda sig av begreppet informationssäkerhet. En mer framkomlig väg har vissa gånger visat sig vara att diskutera en specifik fråga eller verksamhet utifrån en mer nedbruten ansats när det gäller terminologin. Ibland har konfidentialitetsfrågorna hamnat i fokus, ibland har det rört sig om aspekter kopplat till spårbarhetsproblematiken. En annan tendens är att det är enklare att resonera och diskutera utifrån begrepp som cyberbrottslighet och cybersäkerhet än informationssäkerhet, men detta varierar med olika aktörer.

I infosäkutredningens delrapport 2 konstateras att det i Sverige verkar ”finnas ett glapp i begrepp och definitioner mellan en övergripande nivå och den vardag som branschens aktörer och användare använder”.[27] Våra erfarenheter visar att samma förhållande även gäller på den europeiska nivån.

24. Intervju med representant från DG JFS i Bryssel 06-03-13.
25. SOU 2004:32 Informationssäkerhet i Sverige och internationellt – en översikt. Delrapport 2 från InfoSäkutredningen, sidan 17.
26. Ibid.
27. Ibid, sid. 16.

De stora dragen – relevanta aktiviteter och initiativ

Fokus i denna rapport ligger inte på de initiativ och aktiviteter som genomförs inom EU på informationssäkerhetsområdet, utan snarare på de aktörer som är tongivande i denna process. För att skapa en förståelse för hur området utvecklats har vi ändå valt att i stora drag presentera de viktigaste linjerna i det arbete som bedrivits på informationssäkerhetsområdet under de senaste åren. För vidare läsning rekommenderas Infosäkutredningens Delrapport 2[28] och Pär Erikssons FOI Memo ”Kartläggning av EU:s informationssäkerhetsarbete i första respektive andra pelaren”.[29]

I detta och nästa kapitel redovisas studiens kartläggning av centrala aktörer inom EU när det gäller informationssäkerhetsfrågor.

Policyutveckling

Många av de initiativ som har eller har haft inverkan på informationssäkerhetsområdet springer ur EU:s arbete med att skapa ett ”informationssamhälle för alla”. Redan 1999 presenterades ett initiativ (eEurope 2002) som en del av det som kom att omnämnas som ”Lissabonstrategin”. Syftet med denna strategi – och efterföljande initiativ som eEurope 2005 och nu senast i2010 – var att skapa en gynnsam politik för tillväxt som baseras på den potential som ligger i IT och digitaliseringen av det moderna samhället. Initiativet eEurope ska bl.a. öka spridningen av digital teknik, stödja företag som vill etablera sig på Internet, underlätta regelverket för handel över Internet m.m. Naturligtvis utgör informationssäkerhet en viktig aspekt i att uppnå dessa syften. Inom ramen för dessa initiativ får informationssäkerhet ses som en ”möjliggörare” och därmed en motor för att nå ökad sysselsättning och tillväxt inom EU. Några av de mer specifikt informationssäkerhetsrelaterade aspekter som tas upp i dessa initiativ rör ett billigare, snabbare och säkrare Internet (stort fokus har legat på

28. Not 24, sid. 100 ff.
29. FOI Memo (september 2004), ”Kartläggning av EU:s informationssäkerhetsarbete i första respektive andra pelaren”, Pär Eriksson.

bredbandsfrågan), behovet av att bygga ett ökat förtroende för den elektroniska handeln, säkrandet av en informationsinfrastruktur, krav på skydd av den personliga integriteten m.m.

Den politik som EU för inom IT-området behandlas inte som ett separat område inom EU:s fördrag, utan ingår i stället som en del i fördraget om den inre marknaden, transportpolitik och FoU. Detta medför i sig att ett stort antal aktörer är involverade i frågeställningar som är relevanta för denna studie.

Kopplat till de mer övergripande initiativen och strategierna finns ett antal specifika stödprogram inom eEurope och i2010 varav följande är intressanta ur ett informationssäkerhetsperspektiv:

Safer Internet Plus

EU inrättade handlingsplanen ”Safer Internet Plus” i syfte att hindra spridningen av olagligt, skadligt och rasistiskt material på Internet och främja en gynnsam utveckling av Internetbranschen på europeisk nivå. Den nuvarande handlingsplanen gäller åren 2005–2008.

eTEN

eTen syftar till att utveckla nya transeuropeiska e-tjänster och förbättra deras kvalitet, pålitlighet och säkerhet. Programmet föreslås under 2007 att övergå i ramprogrammet för ”Competitiveness & Innovation” (CIP).

IDABC

IDABC (och dess föregångare IDA) syftar till att skapa förutsättningar för utbyte mellan offentliga administrationer inom EU. I detta sammanhang har bl.a. frågor av interoperabilitetskaraktär behandlats liksom frågan om kvalificerade digitala signaturer.

IST Research

Det finns ett speciellt forskningsspår (IST, Information Society Technologies) inom EU:s ramprogram[30] för att stödja uppfyllandet av visionerna inom eEurope och i2010-strategierna ur ett mer tekniskt utvecklingsperspektiv.

Förutom ansatserna ovan som mer syftar till att skapa tillväxt finns det ett antal som är mer ”säkerhetsorienterade”. Lite grovt kan dessa initiativ kategoriseras efter tillhörigheten i antingen ”cyberbrottslighet”, ”cyberförsvar” eller ”skydd av kritisk informationsinfrastruktur ”. I det förstnämnda fallet återfinns exempelvis det arbete som kommissionen publicerade 2001: ”Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet”.[31] I detta arbete togs ett brett grepp om informationssäkerhetsfrågorna och man beskrev

30. För mer information om EU:s ramforskningsprogram se avsnitt Initiativ kopplade till forskning och utveckling.
31. KOM/2000/890, ”Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet”.

både hot och möjligheter i informationssamhället, inklusive olika former av datorrelaterad brottslighet. Initiativ som faller inom detta område (cyberbrottslighet) riktar sig oftast mot något av de följande:

- integritetsbrott
- innehållsrelaterade brott (exempelvis barnpornografiska brott)
- ekonomisk högteknologisk brottslighet (bedrägerier, spionage, spridning av illasinnad kod)
- brott mot intellektuella rättigheter (upphovsrättsfrågor).

I nuläget förbereds ett nytt meddelande inom cyberbrottlighetsområdet.[32]

Inom ”cyberförsvar”-domänen är det tunnsått med initiativ eftersom dessa faller inom den andra pelarens verksamhet och frågor som rör försvarsområdet ofta tenderar att hamna på de enskilda nationernas bord. Det finns dock några undantag. Enligt uppgift (eftersom studien inte inkluderar de mer försvarsinriktade initiativen och aktörerna har detta inte studerats specifikt av projektgruppen) har EU:s militära stab tagit fram ett militärt informationsoperationskoncept för krishanteringsoperationer utanför EU:s gränser. Inom detta koncept definieras informationssäkerhet som en del av informationsoperationerna, liksom ”datanätverksoperationer” (CNO).[33]

Den europeiska säkerhetsstrategi[34] som togs fram 2003 av rådssekretariatet och som antogs i toppmötet samma år handlar i stor utsträckning om hur Europa ska kunna möta dagens komplexa hot, bl.a. hotet från terrorism. I denna strategi nämns inte informationssäkerhet uttryckligen, däremot påtalas att informationsinfrastrukturen är känslig för terrordåd. I det arbetspapper som kommissionen gav ut nästföljande år under rubriken ”European Security Strategy – Fight against Terrorism” finns även där ett avsnitt där behovet av att skydda den kritiska informationsinfrastrukturen betonas.[35] Inom kommissionen arbetar man för närvarande bl.a. med att ta fram ett program för skydd av kritisk infrastruktur (EPCIP), och mycket av det kan sägas komma från arbetet mot terrorism som drastiskt intensifierades efter 11 september-attackerna och bombningarna i Madrid och London. Frågor som dessa hamnar inom både andra och tredje pelarens verksamhet eftersom de berör såväl aspekter av skydd mot externa hot som rättsliga frågor.

32. Om detta kan man läsa i den nyligen publicerade strategin för ett säkert informationssamhälle: ”Dialog, partnerskap och användarinflytande”. KOM 2006/0251 slutlig.
33. Pär Eriksson, (2004), sid. 19.
34. Ett säkrare Europa i en bättre värld – En europeisk säkerhetsstrategi. 2003-12-12.
35. European Security Strategy – Fight against Terrorism, SEC 2004/332, 2004-03-19.

Legala och icke-regulativa ramverk

Kopplat till de mer övergripande strategierna ovan finns ett stort antal legala och icke-regulativa ramverk som tillkommit för att säkerställa uppfyllandet av målen i strategierna och deras genomförande. Nedan nämns några exempel på relevanta förordningar, direktiv och förslag.

Nät- och informationssäkerhet

- 2001/264/EG: Rådets beslut om antagandet av rådets säkerhetsbestämmelser (säkerhetsbestämmelser för hur sekretessbelagd EU-information ska behandlas)
- Nät- och informationssäkerhet – Förslag till en europeisk strategi KOM/2001/0298 slutlig.
- eEurope 2005: Ett informationssamhälle för alla – En handlingsplan inför Europeiska rådet i Sevilla 2002. KOM/2002/0263, slutlig.
- Halvtidsöversyn av eEurope 2005, KOM/2004/0108, slutlig.
- Förslag till Europaparlamentets och rådets beslut om inrättandet av ett flerårigt gemenskapsprogram för att främja en säkrare användning av Internet och ny online-teknik, KOM/2004/91, slutlig.
- Förordning 2004/460/EG om inrättandet av den europeiska byrån för nät- och informationssäkerhet (Enisa).
- i2010 – Det europeiska informationssamhället för tillväxt och sysselsättning KOM/2005/229, slutlig.
- En strategi för ett säkert informationssamhälle – dialog, partnerskap och användarinflytande. KOM 2006/0251 slutlig.

Cyberbrottslighet (och terrorism)

- Rådets rambeslut om bekämpning av bedrägerier och förfalskningar som rör andra betalningsmedel än kontanter. KOM/1998/0395, slutlig.
- Beslut om bekämpning av barnpornografi på Internet, 2000/375/RIF.
- Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet, KOM/2000/890.
- Konventionen om Internetrelaterad brottslighet, 2001-11-23.
- Förslag till rambeslut om angrepp mot informationssystem, KOM/2002/0173.
- Rådets rambeslut om bekämpandet av terrorism 2002/475/RIF.

Integritet, skydd av personuppgifter och telekomlagstiftning

- Ramlagstiftning för telekommunikationer och uppgiftsskydd direktiv 1995/46/EG och 1997/66/EG.
- Direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer.

- Förordning 2001/45/EG om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.
- Direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation).
- Beslut om utnämning av den oberoende övervakningsmyndighet som föreskrivs i artikel 286 i EG-fördraget (instiftandet av ett uppgiftsskyddsombud och en datatillsynsombudsman), 2004/55/EG (22/12).
- Icke begärd kommersiell kommunikation eller så kallad skräppost (Spam), KOM/2004/0028, slutlig.
- Förslag till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbetet och straffrättsligt samarbete, KOM/2005/0475, slutlig.
- Direktiv 2006/24/EG om lagring av uppgifter som genererats i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät (Datalagringsdirektivet).

Skydd av samhällsviktig infrastruktur

- Den europeiska säkerhetsstrategin – kampen mot terrorismen SEC/2004/332.
- Meddelande från kommissionen till Europaparlamentet. Skydd av viktig infrastruktur i kampen mot terrorismen. KOM (2004) 702, 2004-10-20.
- Grönbok om ett europeiskt program för skydd av kritisk infrastruktur, KOM/2005/0576, slutlig.

Initiativ kopplade till forskning och utveckling (FoU)

De forskningsinitiativ och konkreta projekt och studier som finns inom informationssäkerhetsområdet bör betraktas i rätt policykontext, nämligen Lissabonstrategin och den angränsande ambitionen att uppnå målet om att EU 2010 skulle vara ”den största kunskapsbaserade ekonomin”.

Inom EU finns sedan många år de så kallade ramforskningsprogrammen. I nuläget rullar det sjätte programmet, men redan 2007 är det dags för nästa program som till skillnad från sina föregångare kommer att löpa under en längre tidsrymd, från 2007 till 2013. Inom ramen för dessa program återfinns olika tematiska områden, och inom dessa bedrivs både forskningsprojekt och s.k. SSA-projekt som inte har någon tydlig teknisk utvecklingsprofil. I det nu pågående programmet finns det tematiska området ”IST, Information Society Technologies” där bl.a. frågor kopplade till informationssäkerhetsområdet finns representerade. Budgeten för detta område är drygt 3,6

miljarder euro.[36] Inom området finns forskningsprojekt som behandlar så vitt skilda frågor som biometri, integritetsfrågor och smarta kort.

Nytt för det sjunde ramforskningsprogrammet, dvs. nästföljande program, blir skapandet av ett nytt tematiskt forskningsområde inriktat på europeisk säkerhetsforskning. Som en förberedelse inför denna lansering etablerades ett förberedande program kallat PASR (Preparatory Action for Security Research) för perioden 2004–2006. Syftet med detta förberedande program har i mångt och mycket varit att underlätta nätverkande och etablerande av konsortier inom just säkerhetsforskningsområdet för att på så vis skapa en grund inför starten av det sjunde ramforskningsprogrammet. 2004 antogs 12 stycken forskningsansökningar och 2005 13 stycken. Inom ramen för de projekt som fick finansiering under 2004 års omgång finns bl.a. ett ännu pågående projekt – VITA – med inriktning mot skydd av kritisk infrastruktur. Detta projekt är intressant ur ett informationssäkerhetsperspektiv. I skrivande stund har ansökningsomgången för 2006 precis gått ut och besked väntas under andra halvan av 2006.

Sett ur ett forskningsorganisatoriskt perspektiv finns det ett stort antal aktörer som har ansvar för frågor kopplade till informationssäkerhetsområdet. Eftersom effektivitet är ett ledord finns en uttalad ambition från kommissionens sida att undvika överlappningar mellan olika aktörers verksamheter. Av denna anledning koordineras arbetet inom exempelvis generaldirektoratet för informationssamhälle och medier (med forskning kopplad till exempelvis IST-området), generaldirektoratet för näringsliv och industri (där bl.a. PASR-arbetet återfinns i dag och säkerhetsforskningen med inriktning på rymd och säkerhet kommer att finnas under ramprogram 7) och aktörer som EDA (European Defence Agency) som också bedriver relevant forskning. En annan aspekt kopplad till effektivitetsambitionen är möjligheten till gemensamma utlysningar av forskningsmedel. Detta är något som diskuteras bl.a. mellan aktörer med ansvar för PASR och ICT-forskningen (ICT svarar mot den svenska benämningen IKT som står för Informations- och kommunikationsteknik) inom respektive berörda generaldirektorat inför FP7.

Under det kommande ramprogrammet (FP7) kommer huvuddelen av de forskningsprojekt som är intressanta ur ett informationssäkerhetsperspektiv troligtvis att ligga under DG InfSo:s verksamhet, även om projekt inom säkerhetsforskningsprogrammet kommer att beröra exempelvis frågor av relevans för området skydd av kritisk infrastruktur. En genomgång av de tematiska prioriteringarna inför FP7 visar att område nr 3, ”Information

36. http://cordis.europa/fp6/ist.htm 06-06-28.

and Communication Technologies", uppskattningsvis kommer att få 12,7 miljarder euro under en sjuårsperiod medan säkerhetsforskningsprogrammet inom ramen för "Space and Security" under samma period kommer att få drygt 3,9 miljarder euro.[37]

37. http://cordis.europa/fp6/ist.htm 06-06-28.


find...
Ctrl+F

Vem gör vad? Aktörer i fokus

Detta kapitel utgör kärnan i kartläggningsstudien. Nedan följer en övergripande genomgång av de EU-aktörer som identifierats som intressanta för denna studie. Förutom en mer generell beskrivning av de olika aktörernas verksamhet görs även en djupdykning i mer specifika informationssäkerhetsrelaterade frågor kopplade till de respektive aktörernas verksamhet. I vissa fall har en länk till svenska aktörer identifierats och då anges detta. Avsaknaden av en tydligt utpekad kontaktyta ska dock inte tas för absolut utan kan mycket väl bero på att vi inte hunnit ”gräva djupare” i de svenska aktörernas (främst myndigheters) kontaktytor.

EU-kommissionen

Som tidigare nämnts är det EU-kommissionen som tar initiativ till och utarbetar nya rättsakter för unionen. I frågor som rör den första pelarens verksamhet har kommissionen dessutom en extra stark roll som ensam initiativtagare till politiken. Frågor som rör informationssäkerhetsområdet berör verksamheten för i stort sett alla generaldirektorat. Nedan finns en summering som utgår från relevanta generaldirektorats verksamheter.[38]

Generaldirektoratet för energi och transport

Verksamhet: Transport och energi är av tradition viktiga områden för EU:s politik. I stort syftar denna politik till att ”skapa en hållbar rörlighet som både främjar EU:s konkurrenskraft och medborgarna, skapar högre säkerhet och trygghet och ökade rättigheter”.[39] På generaldirektoratets bord ligger frågor som bland annat rör infrastruktur samt säkerställandet av de ökande säkerhetskraven (som i mångt och mycket drivs av globala utmaningar).

38. Vi har här valt att enbart presentera de generaldirektorat som är av mer betydande relevans ur ett informationssäkerhetsperspektiv. Det kan finnas verksamhet inom andra generaldirektorat som rör informationssäkerhet, men inte av sådan relevans att vi har prioriterat att ta upp det här.
39. Citatet är hämtat från en beskrivning av generaldirektoratets och generaldirektörens uppdrag. http://cc.europa.eu/dgs/energy_transport/matthias_ruete/mission_sv.html 2006-05-22.

Infosäk i fokus: Det finns ett antal intressanta projekt och initiativ som rör informationssäkerhetsområdet. Ett av dessa är det s.k. Galileoprojektet. Detta projekt, eller snarare de säkerhetskrav som detta projekt kommit att ställa på inblandade parter och andra EU-aktörer, har kommit att driva det interna informationssäkerhetsarbetet framåt. EU har en högre informationssäkerhet i dag mycket tack vare Galileoprojektet.[40]

Ett annat relevant arbete är det som generaldirektoratet är inblandat i kring framtagandet av ett europeiskt program för skydd av kritisk infrastruktur (EPCIP). Där arbetar företrädare för generaldirektoratet nära tillsammans med exempelvis generaldirektoratet för rättvisa, frihet och säkerhet som leder det övergripande arbetet. I nuläget har ett par studier initierats i syfte att undersöka den europeiska kritiska infrastrukturen inom transport- och energiområdet. Studierna syftar till att

- utveckla kriterier för att identifiera europeisk kritisk infrastruktur inom de aktuella sektorerna
- inventera befintlig kritisk infrastruktur
- föreslå allmänna åtgärder som kan vidtas för att öka skyddsnivåerna inom dessa infrastrukturer.[41]

Generaldirektoratet för forskning

Verksamhet: I uppdraget ligger utvecklandet av EU:s policy inom området forskning och teknisk utveckling, koordinerandet av EU:s forskningsrelaterade aktiviteter, stödjandet av unionens policyutveckling inom andra områden (som miljö- och hälsoområdet) samt främjandet av en ökad förståelse för vetenskapens roll i moderna samhällen.[42] Ett redskap i uppfyllandet av uppdraget är de fleråriga ramforskningsprogrammen. Genom dessa kanaliseras finansieringen till relevanta forskningsprojekt och man stärker samverkan mellan olika aktörer inom forskningssektorn. Det nuvarande programmet löper 2002–2006 och har en budget på 17,5 miljarder euro.[43] Generaldirektoratet arbetar nära andra aktörer inom kommissionen, t.ex. det gemensamma forskningscentrat, generaldirektoraten för informationssamhälle och media, transport och energi, miljö, näringsliv och industri – samtliga aktörer med ett uttalat ansvar för forskningsfrågor.

Gemensamma forskningscentrat (JRC)[44]

Verksamhet: RC är en forskningsbaserad policystödjande verksamhet under kommissionen. Organisatoriskt är

40. Intervju med representanter från GD för energi och transport i Bryssel 2006-03-29.
41. http://ec.europa.eu/dgs/energy_transport/security/infrastructures/studies_en.htm 20060522.
42. http://ec.europa.eu/dgs/research/index_en.html 2006-05-22.
43. Ibid.
44. Det gemensamma forskningscentrat har en lite udda organisatorisk roll som både ett generaldirektorat under kommissionen och som en egen myndighet. I denna rapport presenteras JRC:s verksamhet under kommissionen, men den hade dock lika gärna kunnat ha sin ”hemvist” under avsnittet om myndigheter.

det uppdelat i sju geografiskt spridda institut. Arbetet består av forskning av direkt relevans både för de europeiska medborgarna och för industrin. Vidare ägnar man sig åt direktstöd till olika generaldirektorat under kommissionen samt konkurrensinriktade aktiviteter inom ramen för strategiska allianser med externa aktörer (hemmahörande i näringslivet eller inom vetenskapssamhället). JRC spelar dessutom en viktig roll i framtagandet av den europeiska forskningsagendan (ERA).[45]

Infosäk i fokus: Förutom elva prioriterade teman (inför och under FP6) har JRC även identifierat ett antal prioriterade tvärsektoriella frågeområden – så kallade ”cross-sectoral priorities”. Inom ramen för dessa finns bl.a. aspekter med koppling till cybersäkerhet. Forskning av relevans för cybersäkerhetsområdet bedrivs huvudsakligen vid två av JRC:s institut: IPSC (Institute for the Protection and the Security of the Citizen) i Ispra, Italien, och IPTS (Institute for Prospective Technological Studies) i Sevilla, Spanien.

På IPSC:s hemsida framgår att cybersäkerhet utgör en av institutets huvudkompetenser och vid en genomgång av pågående och avslutade projekt med koppling till FP6 återfinns ett antal som har relevans för informationssäkerhetsområdet. T.ex. projektet GRID “A coordination action on ICT vulnerabilities of power systems and the relevant defence methodologies”.[46]

IPTS tillhandahåller strategiskt stöd av teknoekonomisk karaktär i utvecklandet av EU-riktlinjer. Institutet jobbar till största delen med direkta förfrågningar från EU:s institutioner (huvudsakligen kommissionen och parlamentet). Organisatoriskt är institutets verksamhet uppdelad i fyra forskningsenheter, varav en utgörs av ICT (Information and Communication Technologies). Inom ramen för denna forskningsenhet har man drivit projektet ”Privacy and Identity in the Information Society” (FP6 4322), ett projekt inom sjätte ramprogrammets ramar. Även studier inom biometriområdet återfinns inom enhetens verksamhet, liksom studier kopplade till forskningsområdet digital territorialitet.[47]

Generaldirektoratet för hälsa och konsumentskydd

Verksamhet: Generaldirektoratets uppgift är att värna medborgarnas hälsa och konsumentmässiga rättigheter. Detta görs genom att ta fram och utveckla relevanta riktlinjer och lagar samt initiera specifika program.[48]

45. www.jrc.ec.europa.eu 2006-05-22.
46. http://ipsc.jrc.cec.eu.int/listfp.php?id=7 2006-05-22.
47. http://cybersecurity.jrc.es/ 2006-05-22.
48. http://ec.europa.eu/comm/dgs/health-consumer/general-info/mission_en.html 2006-05-24.

Infosäk i fokus: Inom den delen som rör konsumentskydd finns ett antal olika initiativ som generaldirektoratet varit inblandande i och som rör informationssäkerhet. I detta sammanhang kan vi t.ex. nämna det s.k. ”E-Confidence Initiative” som lanserades 2000. Initiativet syftade till att skapa gemensamma kriterier för ”god sed” inom e-handelsområdet.[49] Gränsande till detta område finns även arbete kring säkra betalningar via nätet (det ska ses som ett led i uppfyllandet av målen i eEurope-strategin).[50]

Generaldirektoratet har under flera år jobbat nära DG InfSo i frågor som rör digitaliseringen av sjukvården, inom det så kallade ”eHealth-området”. Här återfinns en stor mängd frågor av informationssäkerhetskaraktär, bl.a. elektroniska patientjournaler, tillhandahållandet av hälsotjänster via nätet, telematik m.m.

Svenska offentliga aktörer som arbetar med liknande frågeställningar återfinns bl.a. vid Socialstyrelsen.[51]

Generaldirektoratet för informationssamhälle och medier

Verksamhet: Generaldirektoratet spelar en nyckelroll i uppfyllandet av Lissabonstrategin, och den vision om Europas ekonomi som världsledande ur ett konkurrensperspektiv som presenterades däri. Enligt verksamhetsbeskrivningen har generaldirektoratet till mål att bl.a. främja innovation och konkurrenskraft i Europa, liksom att göra IKT-tjänster lättillgängliga för allmänheten.

Infosäk i fokus: Inom ramen för generaldirektoratets verksamhet finns ett stort antal initiativ som rör informationssäkerhetsområdet. DG InfSo har en nyckelroll inom EU när det gäller policy- och forskningsfrågor inom informationssäkerhetsområdet (med inriktning på första pelarens verksamhet). Ett relevant policyområde att nämna i detta sammanhang är området elektronisk kommunikation (eKom) med åtföljande direktiv.[52] Inom det nuvarande ramverket finns informationssäkerhetsrelaterade frågor kring konsumentskydd, integritetsskydd och interoperabilitet, bara för att nämna några exempel. Arbetet med att ta fram en policy mot ”spam” har skett i nära angränsning till eKom-arbetet.[53]

Ramverket rörande eKom-frågorna är i skrivande stund föremål för en översyn. Från svensk sida är det

49. Se exempelvis SEC (2004) 1390, ”Commission Staff Working Document: Consumer Confidence in E-Commerce: Lessons learned from the e-confidence initiative”.
50. http://ec.europa.eu/comm/consumers/cons_int/e-commerce/secur_en.htm 2006-05-24.
51. Läs mer på www.socialstyrelsen.se. På Socialstyrelsens webbplats kan man exempelvis läsa om projektet InfoVU som bl.a. berört frågan om elektroniska journaler och informationssäkerhetsrelaterade frågor.
52. Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), http://europa.eu/scadplus/leg/sv/lvb/l24216a.htm 2006-06-29.
53. Fighting Spam http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm 2006-06-15.

Näringsdepartementet som ansvarar för arbetet.[54]

Ett annat relaterat spår är det arbete som bedrivs inom cybersäkerhetsområdet. I slutet av maj 2006 släpptes den nya strategin för ett säkert informationssamhälle. I denna strategi påtalas bl.a. behovet av att adressera dessa frågor, att det måste ske genom samverkan, och att det finns en plan för hur arbetet med strategin ska fortlöpa. Det talas bl.a. om två planerade meddelanden, ett som rör spionprogram och sabotageprogram, och ett om nya typer av cyberbrottslighet.[55]

Avgränsningen mot exempelvis generaldirektoratet för rättvisa, frihet och säkerhet (DG JFS) är tydlig. Inom cybersäkerhetsområdet ingår inga frågor som rör cyberbrottslighet (eller mer policyorienterade aspekter av CIP/CCIP).[56]

Förutom mer policyinriktade aktiviteter (som exempelvis eKom-direktiven) finns inom generaldirektoratet ett antal olika program som rör informationssäkerhet. Ett av de mer intressanta är det så kallade IST-programmet inom vars ramar ett stort antal relevanta forskningsprojekt och s.k. stödjande aktiviteter (supporting actions) finansierats. Inom ramen för det femte ramprogrammet (FP5) återfanns projekt inom så vitt skilda områden som krypto, PKI (Public Key Infrastructure), biometri, smarta kort mm. I det nu pågående ramprogrammet (FP6) finns ett flertal intressanta projekt, bl.a. ett projekt som syftar till att kartlägga, koordinera och stödja prioriteringen av CIIP-forskning inom Europa (egentligen en s.k. Co-ordinated Action). Projektet kallas för CI2RCO, vilket står för ”the European co-ordination Project on Critical Information Infrastructure Research Co-ordination”.[57]

Generaldirektoratet för inre marknaden och tjänster

Verksamhet: Frågor kopplade till den inre markanden är högprioriterade inom EU. Det faller på generaldirektoratet för den inre marknaden och dess tjänsters bord att ta fram och övervaka införandet av riktlinjer som rör denna. Särskilt utpekade är sektorer som exempelvis

- finansiella tjänster
- elektronisk handel
- copyright och intellektuella rättigheter
- patent m.m.

Infosäk i fokus: Att stödja utvecklingen av elektronisk handel är en central aktivitet i uppfyllandet av de mål som presenteras i de så kallade eEurope-strategierna. Direktivet 2000/31/EG ”Direktiv om elektronisk handel”

54. Intervju med representanter från Näringsdepartementet, 2006-04-12.
55. Se not nr. 32 på sid. 33.
56. Ansvarsfördelningen mellan de olika generaldirektoraten framkom bl.a. vid en intervju med representanter från DG JFS i Bryssel 2006-03-13.
57. IST-2004-15818, läs mer på http://www.ci2rco.org/ 2006-06-30.

behandlar (eller hänvisar) i ett antal paragrafer till frågor av informationssäkerhetskaraktär. Bl.a. tar man upp frågan om skydd för enskilda personer när det gäller behandling av personuppgifter och konfidentialitet vid kommunikation.[58] Det finns även en expertgrupp inom området elektronisk handel.[59] Syftet med denna grupp är att underlätta koordinerandet mellan medlemsstaterna och mellan medlemsstaterna och kommissionen. Gruppen ska även diskutera problem som uppstår i samband med införandet av direktivet samt fånga upp viktiga frågor kopplade till det aktuella området. Från Sveriges sida deltar Konsumentverket i arbetet.[60]

Generaldirektoratet för näringsliv och industri

Verksamhet: Generaldirektoratet arbetar för att främja handeln inom EU och minska befintliga handelshinder. Det ska förbättra konkurrenskraften för den europeiska industrin och skapa en kontinuerlig och hållbar utveckling. Generaldirektoratet arbetar även för att gynna den tekniska utvecklingen samt främja innovationskraft och entreprenörskap.

Infosäk i fokus: Inom generaldirektoratet finns ett antal olika verksamheter där informationssäkerhetsfrågorna på ett eller annat sätt kommer in. Med tanke på den övergripande inriktningen på att främja handel och minimera handelshinder, står standardiseringsfrågorna självklart högt på dagordningen. Det finns en speciell enhet som jobbar med standardiseringsfrågor. Den mest specifika och aktuella standarden inom området är den som vanligtvis hänvisas till som LIS (Ledningssystem för informationssäkerhet). Denna är ursprungligen en brittisk standard, som sedan blivit en svensk, europeisk och internationell ISO-standard. Arbetet med att utveckla denna standard sker inom organisationer som ISO (globalt) och CEN (inom Europa). Naturligtvis finns kopplingar mellan EU:s aktörer som arbetar med standardiseringsfrågor och de olika standardiseringsorganisationerna. Läs mer om de sistnämnda under avsnitt *Övriga aktörer*.

En annan verksamhet som är relevant för denna studie är den som under perioden 2007–2013 föreslås drivas inom det tilltänkta ramprogrammet för konkurrenskraft och innovation (CIP). Ramprogrammet kommer att bestå av tre specifika delprogram, varav det som föreslås kallas ”ICT Policy Support Programme” antagligen kommer att vara mest relevanta ur ett informationssäkerhetsperspektiv. Tanken är att detta program ska bygga på ambitionerna i de tidigare programmen: e-Ten,

58. Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden. (”Direktiv om elektronisk handel”).
59. 2005/752/EG Tillskapandet av en expertgrupp inom området elektronisk handel.
60. http://ec.europa.eu/internal_market/e-commerce/expert-group-members-en.htm 20060524.

Modinis och e-Content.[61] Syftet med delprogrammet är att

- stimulera marknadskonvergens mellan områdena elektroniska nätverk, media (content) och digital teknik
- försöka nå lösningar på problem som i dagsläget fungerar som flaskhalsar för en utveckling av elektroniska tjänster inom unionen
- stödja moderniseringen av den offentliga sektorn i syfte att höja produktiviteten och förbättra tjänsterna.[62]

Inom generaldirektoratet finns även programmet IDABC (”Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens”).[63] Programmet ska förse offentliga förvaltningar, företag och medborgare med alleuropeiska e-förvaltningstjänster. Målet är att öka de europeiska offentliga förvaltningarnas effektivitet och samarbetet mellan dessa. För att uppnå detta utfärdar IDABC rekommendationer, utvecklar tekniska lösningar och tillhandahåller relevanta tjänster liksom bistår med finansiering till olika projekt.[64]

I princip finns två olika typer av projekt inom IDABC. Projekt som

- implementerar gränsöverskridande offentliga tjänster för specifika policyområden
- tillhandahåller gemensamma tjänster eller rekommendationer och gemensam infrastruktur för andra projekt inom IDABC.

Inom ramen för programmet finns ett flertal säkerhetsrelaterade projekt. Förutom den grundläggande alleuropeiska nätverksinfrastrukturen sTESTA som ska tillhandahålla ett säkerhetsackrediterat nätverk, finns bland annat:

- Säkerhetsinstrument.
- CIMS (Common Identity Management Service).
- Certifikatstjänster.
- eID.
- En initial studie kring det ömsesidiga erkännandet av elektroniska signaturer.[65]

Kopplat till IDABC:s verksamhet finns en kommitté, PEGSCO, som bl.a. har synpunkter på verksamheten och inriktningen. Formellt är det kommissionen som fattar beslut i olika frågor.[66] I PEGSCO ingår för Sveriges räkning representanter från VERVA.[67]

I ett tidigare avsnitt om FoU-initiativ inom området (se sida 38) nämndes

61. http://ec.europa.eu/enterprise/enterprise_policy/cip/index_en.htm 2006-05-24.
62. Ibid.
63. Beslut av parlamentet och rådet om IDABC, 2004/387/EG, den 21 april 2004.
64. http://ec.europa.eu/enterprise/ida/index_en.htm 2006-05-30.
65. IDABC Work Programme 2005-2009 (second revision). http://ec.europa.eu/idabc/en/document/5101/3 2006-05-30.
66. Intervju med representanter från IDABC, 2006-03-13.
67. Intervju med representanter från VERVA, 2006-02-15.

PASR, säkerhetsforskningsprogrammet som ska förbereda inför FP7. Rent organisatoriskt har detta program sin hemvist inom generaldirektoratet för näringsliv och industri, och tidigare tillhörde det generaldirektoratet för forskning. Inom ramen för PASR har ett antal forskningsprojekt finansierats som har haft relevans för informationssäkerhetsområdet. Läs mer om dessa projekt på hemsidan.[68]

Generaldirektoratet för rättvisa, frihet och säkerhet

Verksamhet: Generaldirektoratet är det yngsta (1999) och det minsta inom kommissionen. Till dess uppgifter hör att se till att rättvisa, frihet och säkerhet upprätthålls och bevaras inom EU:s gränser. Till skillnad från vad som gäller för andra politikområden – som exempelvis de som berör den inre marknaden – delar kommissionen inom området rättvisa, frihet och säkerhet initiativrätten med de olika medlemsstaterna.

Den rättsliga grunden för generaldirektoratets verksamhet står att finna i Rom- och Amsterdamfördragen. Ett viktigt inriktningsdokument är även slutsatserna från Europeiska rådets möte i Tampere. Generaldirektoratet består av sjutton olika policyenheter uppdelade på fyra direktorat – varav två är relevanta för denna studie:
C och D (Civil Justice, Rights and Citizenship respektive Internal Security and Criminal Justice).[69]

Infosäk i fokus: DG JFS är förutom DG InfSo den aktör inom kommissionen som har det tydligaste ansvaret för frågor kopplade till informationssäkerhetsområdet (frågor som rör den tredje pelarens verksamhet). På generaldirektoratets bord ligger förutom frågor kring cyberbrottslighet, dataskydd och cyberterrorism även frågor kring CIP och CIIP där direktoratet har det övergripande ansvaret. Rent organisatoriskt faller alla aspekter utom dataskydd inom enhet D (se ovan). Dataskyddsfrågor återfinns i stället inom enhet C.

I takt med utvecklingen av EU mot ett informationssamhälle för alla och med en ”gränslös” inre marknad har flödet av personuppgifter mellan EU:s medlemsländer ökat markant. I syfte att undanröja potentiella hinder för sådana flöden och att skydda personuppgifterna har lagstiftningen kring detta område harmoniserats mellan länderna (direktiv 95/46/EG). Direktivet har bl.a. legat till grund för den svenska personuppgiftslagen (PUL) inom vars ram relaterade säkerhetsfrågor beaktas.[70]

Kopplat till området finns en speciell arbetsgrupp, den så kallade artikel 29-gruppen. I gruppens uppgifter ingår att:

68. http://cordis.europa.eu/security/findoc.htm 2006-05-30.
69. http://ec.europa.eu/comm/dgs/justice_home/index_en.htm 2006-05-26.
70. FOI Memo 1017, sid. 11, Pär Eriksson.

- tillhandahålla expertstöd från de respektive medlemsländerna i frågor som rör dataskydd
- främja ett unisont införande av generella principer stadfästa i direktivet genom samverkan mellan respektive länders tillsynsaktörer
- råda kommissionen i frågor som rör den personliga integriteten i processandet av personuppgifter
- utfärda rekommendationer till allmänheten och relevanta institutioner inom dess ansvarsområde.[71]

I artikel 29-gruppen representeras Sverige av Datainspektionens generaldirektör.

Inom DG JFS finns en speciell enhet som arbetar med dataskyddsfrågorna, både utifrån riktlinjerna men även som initiativtagare till studier. I nuläget genomförs en utvärdering av arbetet efter Dataskyddsdirektivets översyn 2002/2003. I översynen konstaterades att inga förändringar i direktivet var nödvändiga men att det däremot fanns ett antal frågor som behövde uppmärksammas vidare. En av dessa är det faktum att Dataskyddsdirektivet inte kan tillämpas inom den tredje pelaren. Eftersom DG JFS anser att det finns ett behov av skydd av personuppgifter även kopplat till tredje pelarens verksamhet har de arbetat fram ett förslag till beslut för rådet. Många medlemsstater är dock kritiska till detta förslag.[72]

Överföring av personuppgifter till länder utanför EU har tidigare varit problematiskt. Grundprincipen är att personuppgifter bara kan överföras om man kan garantera en tillräcklig skyddsnivå. I nuläget finns avtal med Schweiz, Kanada och Argentina som möjliggör överföring av personuppgifter till dessa länder. Enheten arbetar (våren 2006) på avtal med Australien, Nya Zeeland och USA. För överföring till andra länder krävs avtal på organisationsnivå (Contractual Clause). Det är då den part eller organisation med bas i EU som har skyldighet att säkerställa att utlämnade personuppgifter inte används på ett sätt som strider mot EU:s direktiv.

När det gäller frågor om cyberbrottslighet bedrivs den relevanta verksamheten inom enhet D2 (”Fight against economic, financial and cyber crime”). I nuläget pågår verksamhet som är tänkt att utmynna i ett nytt meddelande inom cyberbrottslighetsområdet nästa år.[73]

Inom CIP- och CIIP-området pågår, som tidigare nämnts, ett intensivt arbete kopplat till det så kallade EPCIP-programmet. Initiativet till detta program togs redan 2004 då kommissionen lade fast riktlinjerna för programmet. Efter detta följde under 2005 en process där olika seminarier

71. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf 2006-06-29.
72. Intervju med representant för enhet C5 – Data Protection – vid DG JFS i Bryssel 2006-03-29.
73. Intervju med representanter från enhet D2 – Fight against economic, financial and cyber crime – vid DG JFS i Bryssel 2006-03-13.

hölls och där ett grönpapper om skydd av kritisk infrastruktur togs fram. Ambitionen har varit att lägga fast en politik för CIP och CIIP under 2006, men om detta lyckas återstår att se. Det finns tydliga skillnader mellan olika länders syn på EU:s roll inom detta område och vad politiken ska innehålla. DG JFS har haft det övergripande ansvaret i denna process, även om ett stort antal aktörer inom EU och representanter för EU:s medlemsländer varit inblandade.[74]

Rådet

Som tidigare nämnts för rådet de enskilda medlemsstaternas talan i EU-samarbetet och är dessutom unionens högsta beslutande organ. Rådet granskar och beslutar om kommissionens förslag till rättsakter, initierar egna förslag inom den andra och tredje pelaren, bestämmer tillsammans med parlamentet EU:s budget samt sluter internationella avtal mellan EU och andra stater och organisationer.

Arbetet i rådet bedrivs på tre nivåer: på tjänstemannanivå i olika tematiskt indelade rådsarbetsgrupper, på hög tjänstemannanivå i de ständiga representanternas kommitté (Coreper) som består av medlemsstaternas EU-ambassadörer, och i själva ministerrådet där medlemsstaternas fackministrar träffas. För kontinuiteten i rådsarbetet svarar det s.k. rådssekretariatet som utgör rådets stabsfunktion och som stöttar ordförandeskapet i förhandlingsarbetet. Rådssekretariatets roll och inflytande varierar med ordförandeland – vid ett svagt ordförandeskap stärks rådssekretariatets roll och omvänt.

I denna studie har fokus legat på den verksamhet som bedrivs inom några identifierade och relevanta rådsarbetsgrupper där mycket av arbetet görs, och vissa enheter inom rådssekretariatet. Nedan finns en kortfattad beskrivning av det som framkommit vid de intervjuer som projektgruppen genomfört. Relativt lite information om den ovan nämnda verksamheten finns tillgänglig via Internet eller andra källor.

RÅDSARBETSGRUPPER

Sektorsövergripande arbetsgruppen mot organiserad brottslighet (MDG)

Verksamhet: Den sektorsövergripande arbetsgruppen mot organiserad brottslighet inrättades 1997 och har till uppgift att dra upp riktlinjer för hur kampen mot den organiserade brottsligheten ska samordnas. I övrigt hanteras en rad skiftande frågor av skilda slag.[75]

Informationssäkerhetsrelaterade frågor har varit uppe för behandling

74. Om man utgår från kommissionens process (och DG JFS:s roll i denna) mot framtagandet av ett europeiskt program för CIP. Denna process har ägt rum parallellt med EU:s arbete med att förbättra förmågan att möta och hantera terrorism där även aspekter kopplade till CIP (och andra aktörer) har ingått. Se analys i Pär Eriksson, Svante Barck-Holst, (2005), ”Politik för skydd av kritisk infrastruktur i EU och i Sverige – en jämförande analys”, FOI-R 1793 SE, kapitel tre.
75. http://regeringen.se/sb/d/63331 2006-02-20.

i arbetsgruppen men bara i väldigt begränsad omfattning.[76]

Ansvarigt departement: Justitiedepartementet.

Arbetsgruppen för forskning

Verksamhet: Gruppen ansvarar för utformningen av förslag till rådets beslut om EU:s forskningspolitik. Centralt i denna uppgift står ansvaret för informationsutbyte och förhandlingar inför beslut om EU:s ramprogram för forskning samt EU:s ”forskningspolitiska proposition” som kommer vart fjärde år.[77]

Ansvariga departement: Utbildnings- och Näringsdepartementet.

Arbetsgruppen för telekommunikationer och informationssamhället

Verksamhet: Arbetsgruppen ägnar sig åt frågor om elektroniska kommunikationer och informationssamhällets tjänster. Inom rådsarbetsgruppen diskuteras frågor av informationssäkerhetskaraktär. Utifrån de meddelanden som kommer fram inom området (som de planerade inom exempelvis ”cyber security”-området) kommer rådsarbetsgruppen att medverka till att ta fram rådsslutsatser som kan leda till en agenda för vad som behöver göras inom området.

Ansvariga departement: Näringsdepartementet samt delvis Finansdepartementet, Kulturdepartementet och Jordbruksdepartementet.[78]

RÅDSSEKRETARIATET

Generaldirektorat C, enhet 3A – Inre marknaden, konkurrenskraft, industrin, forskning, energi, transporter och informationssamhället (fri översättning)

Verksamhet: Enheten tillhandahåller processtöd och politisk rådgivning till rådets ordförandeland och de övriga medlemsstaterna så att dessa ska kunna sköta sina arbetsuppgifter. Konkret innebär detta förberedelser inför rådets möten inom områdena post- och telekommunikationer, informationssamhället, multimedia, HDTV och dataskydd. Enheten har haft en central och drivande roll i avtalsskrivandet inför bildandet av Enisa.[79]

Europaparlamentet

Parlamentets huvuduppgift i EU-samarbetet är att fatta beslut och att utöva demokratisk kontroll. Konkret innebär det bland annat att inom vissa politikområden i den första pelaren, tillsammans med rådet, granska och bestämma om kommissionens initiativ till rättsakter kan antas samt att godkänna EU:s budget och kommissionens

76. Intervju med Anna-Carin Svensson, kansliråd vid Justitiedepartementet och kontaktperson för arbetsgruppen. 2006-03-03.
77. http://www.regeringen.se/sb/d/2823 2006-02-20.
78. http://www.regeringen.se/sb/d/6341 2006-02-20 samt intervju med representant vid Sveriges ständiga representation vid Europeiska Unionen 2006-03-14.
79. Intervju med representant för enhet 3A i Bryssel 2006-03-13.

sammansättning. Parlamentet har ingen beslutfattande roll i den andra och tredje pelaren men ska vanligtvis hållas informerad om de beslut som fattas.

Parlamentets utskott

Som tidigare nämnts har fokus för studien varit på kommissionens verksamhet (och i viss mån den som bedrivits inom ramen för rådsarbetsgrupperna) eftersom denna är viktig i ett initialt skede och det är där som svenska myndigheter har störst möjlighet till påverkan. Därför har projektgruppen valt att inte lägga någon större vikt vid parlamentets verksamhet.

Det som gjorts är en kort genomgång av parlamentets utskott, särskilt *utskottet för inre marknad och konsumentskydd samt utskottet för medborgerliga fri- och rättigheter*. I båda dessa utskott behandlas frågor som är relevanta för informationssäkerhet. Ett konkret exempel är direktivet om lagring av trafikdata som har antagits av ministerrådet och Europaparlamentet och som behandlades inom ramen för utskottet för inre marknad och konsumentskydd.[80]

Myndigheter

Andra centrala aktörer i EU-samarbetet är de EU-myndigheter (ibland kallas dessa för gemenskapsbyråer) som har inrättas som kompetenscentrum inom olika områden. Dessa är vanligtvis organisatoriskt nära knutna till kommissionen.

Som tidigare påtalats har JRC, det gemensamma forskningscentrat, en dubbel roll som både en myndighet och ett generaldirektorat under kommissionen. I denna framställning återfinns JRC under den beskrivning av kommissionens verksamhet som inledde detta kapitel.

Europeiska nät- och informationssäkerhetsbyrån (Enisa)

Verksamhet: I början av 2005 sjösattes den europeiska myndigheten för nätverks- och informationssäkerhet (Enisa – European Network and Information Security Agency).[81]
I Enisas uppgift ligger att stödja kommissionen, medlemsstaterna och representanter från ”företagsvärlden” i arbetet med att möta de krav som finns på nätverks- och informationssäkerhet, utifrån både befintliga och kommande lagar och regelverk. Enisa utgör alltså ett expertorgan där medlemsstater och institutioner inom EU kan söka råd kring informationssäkerhetsfrågor.[82]

Arbetet inom Enisa har följande fokus:

- Ge *råd och stöd* till Kommissionen och medlemsländerna inom olika områden (inklusive forskning).

80. Intervju.
81. 460/2004/EG, 10 mars 2004.
82. http://enisa.eu.int 2006-05-30.

- Stödja metodutveckling och genomförandet av *riskanalyser och riskhantering*.
- Verka för *medvetandehöjande åtgärder och samverkan* mellan olika aktörer (public-private partership).[83]

Eftersom Enisa är en relativt ny myndighet återstår en del för att nå målsättningarna. Hittills har en stor del av kraften gått åt till att bygga upp myndigheten och inte minst rekrytera personal. Uppskattningsvis kommer myndigheten att bestå av 44 stycken medarbetare när den 2006 beräknas vara i fullt arbete.[84]

Från ett svenskt perspektiv kan det vara intressant att känna till att det finns svenska representanter i såväl Enisas styrelse (Fredrik Sand, Näringsdepartementet) som i intressentgruppen (Sead Muftic vid KTH och Magnus Nyström vid RSA Security).[85]

Verksamheten kommer att utvärderas 2007.

Decentraliserade organ

Europeiska polisbyrån – Europol

Verksamhet: Europol är EU:s polisbyrå, ett organ för behandling och analys av underrättelser som rör organiserad, gränsöverskridande brottslighet inom EU. Arbetet baseras uteslutande på information som Europol får från medlemsländernas polisbyråer. Förutom att Europol hjälper medlemsländerna med analyser bistår de även med att utreda specifika brottsliga verksamheter som rör minst två medlemsländer. Som organisation har Europol inga operativa befogenheter vilket innebär att de inte har rätt att anhålla, förhöra eller spana på misstänkta brottslingar. De kan inte heller bedriva förundersökningar eller andra formella brottsutredningar.[86]

Europol består av tre huvudavdelningar:

- Avdelningen för information och teknologi
- Avdelningen för allvarlig brottslighet (Serious Crime)
- Avdelningen för ledning och styrning (Corporate Governance).[87]

För denna studie är enheten för högteknologisk brottslighet, som organisatoriskt befinner sig under avdelningen för allvarlig brottslighet, den som är mest relevant.

Infosäk i fokus: I december 2001 vidgades Europols mandat och frågan om högteknologisk brottslighet hamnade på prioriteringslistan. Tidigt nästföljande år startades enheten för högteknologisk brottslighet (HTCC – High

83. www.enisa.eu.int/pages/0103.htm 06-06-28.
84. Work Programme 2005, "Information Sharing is Protecting", Ref: MB 2005/02.
85. www.enisa.eu 2006-06-19.
86. Information hämtad från EU-upplysningens http://www.eu-upplysningen.se och från Europols hemsida www.europol.eu.int 2006-05-31.
87. www.europol.eu.int/index.asp?page=orgchart 06-06-28.

Tech Crime Unit). HTCC tillhandahåller operativt stöd till medlemsländerna och till enheterna inom Europol men står även för mer strategiska analyser (hotbedömningar när det gäller datarelaterad brottslighet), utbildning och deltagande i olika arbetsgrupper och konferenser.[88]

På HTCC:s bord hamnar frågor där datorer antingen utsätts för eller används vid en cyberattack. Detta leder till att bl.a. följande frågor och brott är aktuella:

- Hacking
- Spam
- Illasinnad kod
- E-bedrägeri
- Pengatvätt
- Barnpornografi
- e-terrorism
- Identitetsstöld m.m.

Från svensk sida är det främst Rikskriminalpolisen som står för kontaktytorna gentemot HTCC.

Eurojust

Verksamhet: Eurojust är ett relativt nyskapat organ (2002) för straffrättsligt samarbete mellan medlemsstaterna. Deras verksamhet finansieras via EU:s budget. Eurojusts uppgift består i att underlätta och förbättra samordningen av brottsutredningar och åtal som rör flera medlemsländer. Organisationen utgörs av 25 stycken nationella medlemmar, en från varje EU land, som är åklagare, domare eller polistjänstemän med motsvarande behörighet.[89]

Infosäk i fokus: Eurojust har möjlighet att agera när ett brott är gränsöverskridande och uppfyller kriterierna för ett antal specificerade brott. Ett av dessa brott är databrottslighet. Eurojust har således möjlighet att agera inom det område som är relevant för denna studie.

The European Union Institute for Security Studies (ISS)

Verksamhet: ISS är ett oberoende institut som skapades år 2001 och ska närmast ses som en tankesmedja. Som framgår av beslutstexten från tillskapandet av institutet är dess främsta uppgift att ”assist the implementation of the Common Foreign and Security Policy (CFSP) and in particular of the European Security and Defence Policy (ESDP)”.[90]

Som ett fristående och oberoende institut företräder eller försvarar inte ISS några nationella intressen. Detta är en viktig utgångspunkt för ISS som ska verka för en gemensam europeisk säkerhetskultur, berika den strategiska debatten kring intressanta och relevanta frågor, och arbeta för att systematiskt sätta unionens intressen i fokus.[91]

88. Intervju med representanter från HTCC i Haag, 2006-03-30.
89. http://www.eurojust.eu.int samt http://www.eu-upplysningen.se 2006-05-31.
90. Council Joint Action av den 20 juli 2001 angående skapandet av Europeiska Unionens institut för säkerhetsstudier. 2001/554/CFSP.

Infosäk i fokus: Av naturliga skäl finns det i sig inget fokus inom ISS på informationssäkerhetsfrågor. Däremot har institutet bl.a. arrangerat ett seminarium (2004) med titeln ”Information technology Security in the 21st Century: Implications for the EU”. Vid seminariet deltog en inbjuden grupp analytiker med varierande expertis och bakgrund, som diskuterade IT-relaterade säkerhetsfrågor och möjliga implikationer för EU. Ambitionen var att

- belysa potentiella säkerhetsrisker kopplade till IT-beroende infrastrukturer
- utforska kopplingen mellan IT och kritisk infrastruktur ur ett beroendeperspektiv (såväl direkt som indirekt)
- sammanföra en grupp analytiker i syfte att dra uppmärksamhet till IT-säkerhetsfrågorna.[92]

Inom institutets ramar har det även publicerats ett så kallat ”Chaillot paper” av relevans för informationssäkerhetsområdet: ”Information security – a new challenge for the EU”.[93]

Övriga aktörer

Standardiseringsorganisationer

Standardisering är en viktig fråga, inte enbart inom EU utan även betraktat ur ett globalt perspektiv. Standarder underlättar vårt vardagliga liv men de utgör också viktiga förutsättningar för företagande inom och utanför unionens gränser. Det finns ett antal olika standardiseringsorganisationer varav en del är verksamma i en global kontext, och andra på en europeisk eller nationell nivå. Viktigt att nämna i detta sammanhang är att det finns en tydlig koppling mellan det arbete som de olika organisationerna bedriver, och det tillhör snarare regel än undantag att en nationell standard blir en europeisk standard och sen kanske även en internationell standard – eller tvärt om. Oftast finns det alltså inga vattentäta skott mellan de olika organisationernas verksamheter.

På den europeiska arenan finns det i huvudsak tre standardiseringsorganisationer:

- **CENELEC** (European Committee for Electrotechnical Standardization). Arbetar med standardiseringsfrågor kring elektroteknik.

91. Information delvis hämtad från ISS hemsida: www.eu-iss.org 2006-06-19.
92. Information om seminariet och en sammanställning av resultaten från detta står att finna på http://www.iss-eu.org.
93. Chailllot Paper Nr. 76, (mars 2005), ”Information Security – A New Challenge for the EU”, författat av: Alain Esterle, Hanno Ranck och Burkard Schmitt. Kan laddas ner från http://www.iss-eu.org/public/content/chaile.html 2006-05-30.

- **CEN** (European Committee for Standardisation) Arbetar med ett stort antal frågor varav en del faller inom ramen för informationssäkerhetsområdet.
- **ETSI** (European Telecommunications Standards Institute) Fokus på telekommunikationsfrågor.

Vissa frågor har sin naturliga hemvist och upprinnelse ur ett standardperspektiv på den europeiska arenan, medan andra mer hör hemma i en global miljö. Informationssäkerhetsfrågorna är av den senare karaktären, medan frågor som exempelvis har att göra med byggnadsindustrin tenderar att vara mer lokala (i den här meningen en fråga för EU-nivån). Informationssäkerhet är inte en fråga som enbart är av betydelse för EU och föga förvånande sker en stor del av arbetet på den internationella nivån inom ramen för ISO (International Organisation for Standardisation). Där finns det ett antal arbetsgrupper som bl.a. arbetar med att utveckla befintliga standarder inom informationssäkerhetsområdet (kopplat till LIS – ISO/IEC 17799).

Från svensk sida är aktörer som SIS och Swedac (Styrelsen för ackreditering och teknisk kontroll) viktiga aktörer både i det nationella, europeiska och globala standardiseringsarbetet. Representanter från dessa organisationer sitter med i olika arbetsgrupper på såväl europeisk som global nivå och finns även representerade i styrande positioner. Exempelvis sitter vd:n för SIS, Lars Flink, som vice ordförande för det tekniska spåret i CEN.[94]

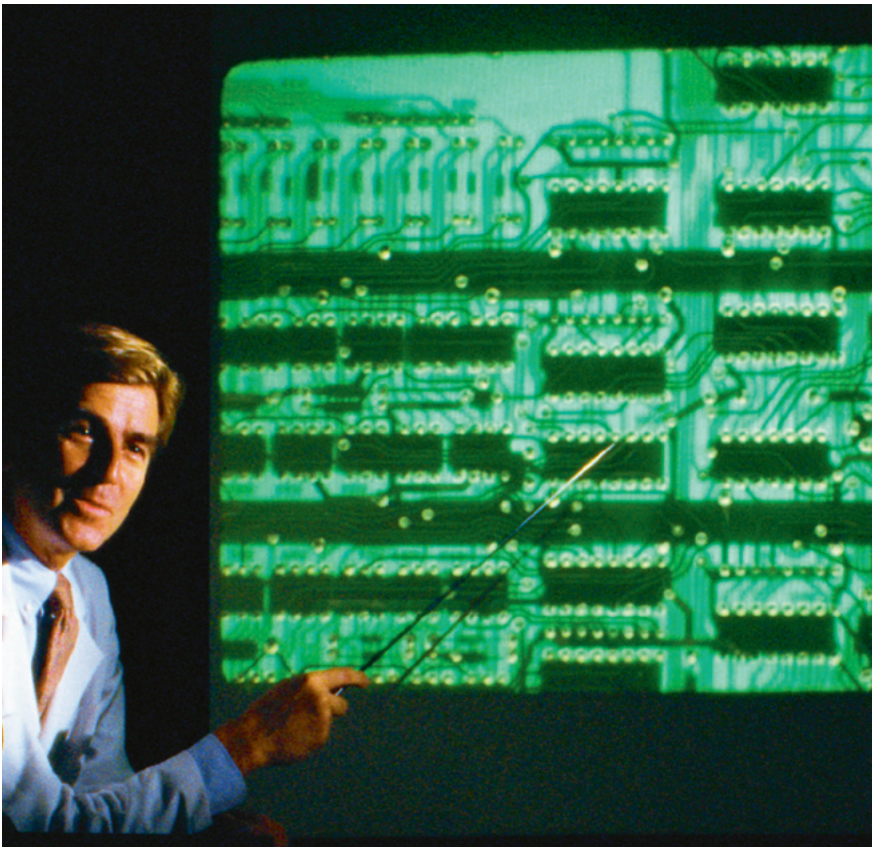
CNSA – Contact Network for Spam Authorities

CNSA är något så intressant som ett nätverk och ett avtal om europeiskt samarbete mot spam som EU-kommissionen tagit initiativ till. CNSA omfattar myndigheter med tillsynsansvar över artikel 13 i direktivet om integritet och elektronisk kommunikation. Artikeln förbjuder näringsidkare att skicka e-postreklam (Spam) till fysiska personer om inte personerna på förhand samtyckt till att få marknadsföring eller det finns ett redan etablerat kundförhållande.[95]

CNSA hanterar huvudsakligen spamfrågor men agendan beror även av vilka frågor de olika medlemsstaterna prioriterar. Kommissionen är drivande i gruppen. Exempel på närliggande frågor som behandlas i CNSA är Botnets, spyware och överbelastningsattacker.

Gruppen fungerar som ett forum för informationsutbyte där erfarenheter utbyts på ett strukturerat sätt. Forumet erbjuder möjligheter för deltagande myndigheter att knyta kontakter och skapa nätverk. Det finns även möjlighet att informera de andra medlemsstaterna om den verksamhet som bedrivs på en

94. Intervju med Swedac 2006-02-23, samt med SIS 2006-04-18).
95. Konsumentverkets webbplats (2006-06-15) http://www.rattsinformation.konsumentverket.se/mallar/sv/artikel_datum.asp?lngCategoryId=977&lngArticleId=4644.



nationell nivå och om frågor som man tycker är viktiga ur det egna landets perspektiv.

Sverige representeras i CNSA av Konsumentverket, men även PTS deltar ibland och tillhandahåller teknisk expertis inom vissa frågor.[96]

Lobbyistorganisationer

Lobbyistverksamhet syftar till att påverka beslutsfattare. Inom EU finns ett stort antal företrädare för olika intresseorganisationer, konsumentgrupper mm. som har organiserat sig i olika formationer för att försöka påverka beslutsfattandet inom EU. För

96. Intervju med representanter från PTS 2006-02-07.

lobbyverksamhet som riktar sig mot kommissionen respektive Europaparlamentet finns det tydliga regler för hur samrådet ska ske med lobbyister.

Enligt EU:s fördrag bör kommissionen, innan ny lagstiftning föreslås, samråda med olika intressenter. Detta kan ske på olika sätt – skriftligen, muntligen, via Internet etc. vilket öppnar upp för alla de organisationer, och för allmänheten, som inte finns formellt representerade i exempelvis kommissionens expertgrupper.

När det gäller ministerrådets verksamhet finns det inga särskilda regler för hur lobbyister och intressegrupper får eller bör agera. Däremot är det så att den lobbying som sker mot ministerrådets verksamhet i första hand tar fokus på nationell nivå där man försöker påverka medlemsländernas regeringar (ministerrådet företräder nämligen medlemsländerna och deras intressen).[97]

För denna studie har vi inte gjort någon undersökning av specifika lobbyistorganisationer och deras verksamhet. Däremot har en snabb sökning av registrerade så kallade konsultativa aktörer (inklusive lobbyistorganisationer) gjorts. För den som är intresserad av att veta mer om EU:s konsultativa förfarande och vilka aktörer som formellt ingår i detta samt vilka övriga organisationer som kan vara relevanta rekommenderas kommissionens databas CONECCS.[98]

97. EU-upplysningen – Regler för lobbyister i EU http://www.eu-upplysningen.se/templates/EUU/standardRightMenuTemplate____2862.aspx 2006-04-11.
98. Databasen finns på http://ec.europa.eu/civil_society/coneccs/index-en.htm 2006-06-13.

Diskussion och slutsatser

Nedan presenteras observationer som gjorts under studiearbetet. Varje observation följs av en diskussion där observationen analyseras och slutsatser dras.

Informationssäkerhet – en fråga som skär genom hela samhället

Observation: Informationssäkerhet är en fråga som berör alla. Oavsett om fokus är på den enskilda medborgaren, små eller stora företag eller den offentliga sfären är informationssäkerhet en angelägen fråga. I grunden handlar informationssäkerhet om att säkra viktig information mot externa och interna hot. Informationssäkerhet handlar dock lika mycket om tillit till den teknik som möjliggör affärsvisioner, ekonomisk tillväxt osv. I takt med den ökade användningen av IT i samhället och dess stödjande infrastruktur har informationssäkerhet dessutom kommit att bli en fråga av säkerhetspolitisk dignitet, eftersom den IT-infrastruktur som kan hotas med ”IT-vapen” måste ses som ett nationellt och internationellt intresse.

Diskussion och slutsatser: Med tanke på sakfrågans karaktär är informationssäkerhet en fråga som av nödvändighet faller på många aktörers bord – på nationell, europeisk och internationell nivå. Inom EU innebär detta att vissa frågor, hemmahörande inom exempelvis första pelaren, hanteras av aktörer med den inre marknaden i fokus (informationssäkerhet ses här gärna som en motor i uppfyllandet av målen i eEurope-strategierna) medan andra aktörer tar hand om frågor som faller inom den andra och tredje pelarens verksamhetsområden.

Detta innebär att frågor som rör informationssäkerhet återfinns inom många generaldirektorats verksamhet. Den verksamhet som kommissionen bedriver kan även sägas ha sin motsvarighet inom rådet, som har till uppgift att granska och besluta om kommissionens förslag. Inom vissa politikområden, inom exempelvis första pelaren, delar rådet dessutom sina uppgifter med parlamentet. Sammantaget innebär detta att det självklart finns relevanta frågor hos alla dessa aktörer

(se förra kapitlet för en genomgång av aktörernas verksamheter).

Utöver dessa aktörer berör frågorna även olika myndigheter, som exempelvis Enisa, men även decentraliserade organ som ISS, Europol och Eurojust. Till detta ska läggas ett stort antal intresseorganisationer och lobbyorganisationer, forskningsinstitut (som inte specifikt behandlas i denna studie men ändå bör nämnas), och privata aktörer som exempelvis företag.

Det spridda ansvaret för frågor av informationssäkerhetskaraktär inom EU har även sin motsvarighet nationellt. På många sätt speglar europeiska förhållanden de svenska.

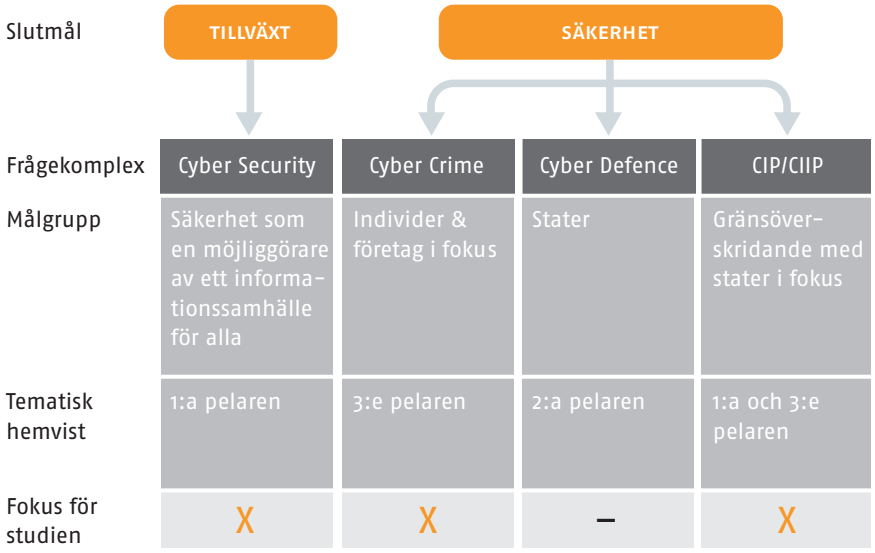
Politik för tillväxt respektive politik för säkerhet

Observation: Inom EU styrs ansvarsfrågan i mångt och mycket av vilket politikområde som frågan har koppling till och inom vilken pelare detta politikområde har sin hemvist. När det gäller informationssäkerhet finns ett betydande överlapp eftersom frågorna skär på tvärs genom många politikområden och dessutom ofta är mångfacetterade (med ekonomiska, tekniska, utrikespolitiska och legala implikationer – bara för att nämna några exempel).

Lite förenklat kan man säga att informationssäkerhetsfrågorna inom EU kan delas in i två politiska huvudspår – *ett där slutmålet är tillväxt och ett där säkerhet i sig står i fokus*. Inom det förstnämnda spåret återfinns säkerhetsaspekter kopplade till informationssamhällets sociala, ekonomiska och tekniska framväxt. Initiativ kopplade till bl.a. eEurope-arbetet återfinns här.[99] I den andra kategorin finns säkerhetsaspekter som rör försvarsfrågor, såsom utvecklandet av EU:s militära informationsoperationskoncept och aspekter som mer kopplas till brottslighet, som exempelvis kommissionens rambeslut om angrepp mot informationssystem. Hit hör även det nu pågående arbetet med att ta fram ett europeiskt program för skydd av kritisk infrastruktur (EPCIP).

Diskussion och slutsatser: Den tydligaste skiljelinjen när det gäller ansvaret är enligt vår bedömning den mellan första och tredje pelarens verksamheter.[100] Förenklat skulle man kunna uttrycka detta som att informationssäkerhetsfrågor som inte har någon koppling till brottslighet faller inom första pelaren, medan frågor med IT-brottsförtecken hamnar inom den tredje pelaren. När det gäller kommissionens verksamhet innebär detta att generaldirektoratet för rättvisa, frihet och säkerhet ansvarar för frågor av IT-brottskaraktär (men även

99. eEurope 2002, eEurope 2005, i2010, m.fl. Läs mer i avsnitt *Policyutveckling*.
100. Med tanke på projektets avgränsningar har verksamheten inom 2:a pelaren inte prioriterats. Detta medför att analysen fokuserats kring verksamheterna i första och tredje pelaren.



Figur 6. *Politik för tillväxt respektive säkerhet.*

CIP). De övriga generaldirektoraten inom kommissionen ansvarar för frågor inom deras respektive politikområden som är av en ”icke-brottslig” karaktär. Många gånger syftar dessa frågor till att skapa förutsättningar för tillväxt inom unionen.

Vid våra intervjuer i Bryssel framkom att generaldirektoratet för informationssamhälle och media samt generaldirektoratet för frihet, rättvisa och säkerhet gjort en uppdelning sinsemellan av vilka frågor som de ska ansvara för. Enligt uppgift faller frågor kopplade till cyberterrorism, CIP och cyberbrottslighet på DG JFS och cybersäkerhet (strategi) på DG InfSo. Även om dessa två generaldirektorat fördelat ansvaret sinsemellan på nämnda vis finns det andra aktörer som också arbetar med frågor kopplade till dessa områden (dock med undantag för cyberbrottslighet). Exempelvis är generaldirektoratet för energi och transport högst inblandade i arbetet med Europeiska programmet för skydd av kritisk infrastruktur (EPCIP).

En annan aspekt som tål att nämnas här är att även om ett enskilt generaldirektorat har tagit på sig en ledande roll inom ett visst frågeområde är det alltid kommissionen som helhet som står bakom ett meddelande när det väl blivit formaliserat. Då ”ägs” inte frågan längre av det enskilda generaldirektoratet som ansvarat för arbetet

med att ta fram underlaget. Under den inledande processen med att ta fram ett relevant underlag samverkar de berörda generaldirektoraten för att koordinera verksamheten och inhämta viktiga synpunkter. Vår uppfattning är dock att insikten om behovet av samverkan generellt är starkare än förmågan att samverka.

Resultatet av EU:s arbete inom informationssäkerhetsområdet

Observation: Som tidigare nämnts (se kapitel tre) resulterar processen där EU:s politik formas i en mängd olika dokument. Innehållet i dessa dokument styr sedan det fortsatta arbetet på europeisk nivå och i de enskilda medlemsstaterna. I de fall det exempelvis beslutats om en ny förordning så träder denna i kraft direkt och på samma sätt i alla medlemsstater.

Generellt sett kan EU:s arbete sägas syfta till (naturligtvis beroende på vilket politikområde som avses) att både reducera sårbarheter och stärka förmågan att hantera kriser (exempelvis kopplat till transnationella infrastrukturer), men även till att skapa förutsättningar för tillväxt och innovation. I de förstnämnda fallen kan EU bidra med att ställa krav på hur medlemsstaterna ska arbeta för att öka säkerheten och hur de kan sköta den nationella beredskapen. De kan även bidra till att stärka säkerheten genom att knyta ekonomiska medel till olika projekt i medlemsstaterna. Slutligen kan EU förmedla information och insatsresurser i en krissituation. När det gäller att skapa förutsättningar för tillväxt och innovation finns t.ex. åtgärder för att minska handelshinder och främja forskning, via exempelvis ramforskningsprogrammen.

Diskussion och slutsatser: Resultatet av EU:s arbete inom informationssäkerhetsområdet kan sammanfattas utifrån följande kategorier:

Strategiska policyinitiativ

Strategiska policyinitiativ återfinns inom såväl området politik för säkerhet som politik för tillväxt, vilka båda nämnts tidigare. I det förstnämnda fallet finns initiativ kopplade till exempelvis kampen mot terrorism och i det andra bl.a. de så kallade eEurope-initiativen.

Direktiv och förordningar

En stor del av EU:s arbete resulterar i olika direktiv och förordningar. Eftersom informationssäkerhet är ett brett område finns det åtskilliga exempel på relevanta direktiv och förordningar. Tidigare i rapporten listades ett antal intressanta legala och icke-regulativ ramverk och exempel gavs inom följande områden:

- *Nät och informationssäkerhet*
  T.ex. Europaparlamentets och rådets förordning nr. 460/2004/EG av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet.

- *Cyberbrottslighet och terrorism*
  T.ex. Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet KOM 2000/890.
- *Integritet och skydd av personuppgifter*
  T.ex. Direktivet om integritet och elektronisk kommunikation, nr. 02/58/EG av den 12 juli 2002.
- *Skydd av kritisk infrastruktur*
  T.ex. Grönbok om ett europeiskt program för skydd av kritisk infrastruktur, KOM 2005/576, 2005-11-17.

Nya aktörer

Skapandet av Enisa kan ses som ett direkt och påtagligt resultat av EU:s arbete inom informationssäkerhetsområdet.

Forskning och relaterade resultat

Det finns ett stort antal forskningsprojekt som antingen har finansierats eller finansieras via EU-medel. I den mån projekten finansieras via ramforskningsprogrammen utmynnar de ofta i nya tekniska lösningar. Givetvis är det de bakomliggande forskningskonsortierna som står som ansvariga för det som projekten mynnar ut i, men det är tack vare EU-finansiering som resultaten kan tas fram. De kan således sägas vara frukterna av ett långsiktigt strategiskt arbete med att säkerställa EU:s tekniska innovationskraft.

Nätverkande

EU:s arbete har gjort att nätverkandet mellan olika aktörer blivit enklare. En del av EU:s verksamhet – exempelvis den som sker inom ramen för Enisa – syftar direkt till att skapa förutsättningar för samverkan mellan olika aktörer. Ibland sker detta dock utan att det är det direkta syftet. Här kan nämnas det konsultativa arbete som ingår i kommissionens initiativfas. I det arbetet deltar ofta ett stort antal aktörer från olika länder, med olika kompetens och hemmahörande inom både den offentliga och den privata sektorn. De kontakter som skapas i dessa sammanhang utgör viktiga redskap i processen men kan även användas av aktörerna för andra syften – exempelvis informationsspridning och informationsinhämtning.

Andra nätverksbefrämjande åtgärder är program såsom eTen och IDABC, där det finns uttalade krav på att projekt som finansieras inom programmen ska främja interoperabilitet och kommunikation mellan länder och organisationer i unionen.

Stora möjligheter till medverkan och påverkan för svenska aktörer

Observation: Flera av våra intervjuobjekt inom EU har uttryckt sig positivt om Sverige och det svenska agerandet i EU. Ofta hänvisas till kompetenta och erfarna experter som i olika sammanhang deltagit i EU-arbetet. Förmågan att bidra brukar lyftas särskilt, till skillnad från enbart förmågan att delta.

Från svenskt håll finns det aktörer med stor erfarenhet av EU:s verksamhet och som under flera år deltagit i EU:s arbete och som har utvecklat ett stort kontaktnät. Dessa aktörer deltar ofta som experter eller i olika kommittéer. Det förekommer även att de sökt och beviljats finansiering via EU:s ramforskningsprogram. När en svensk aktör har ansvar för en fråga med tydlig ”EU-profil” (exempelvis eKom-frågorna) leder det naturligtvis till en omfattande interaktion med relevanta EU-aktörer.

Det finns också en grupp av svenska aktörer som har mer sporadisk kontakt med EU:s aktörer och som har begränsad erfarenhet av direktkontakt med Bryssel, och få eller inga kontakter. Ibland kan detta förklaras med bristen på ett tydligt mandat för agerande på den europeiska nivån, ibland är det bristande kunskap om den roll man skulle kunna spela i EU-sammanhang eller vad man som enskild aktör skulle kunna ”hämta hem”.

Generellt verkar avsaknaden av en genomtänkt och kommunicerad nationell strategi på informationssäkerhetsområdet fungera som en broms för det svenska agerandet i EU-sammanhang. Vilka frågor ska prioriteras? Vilka nationella intressen ska värnas? Vilken typ av information och resultat är viktiga att hämta hem och förmedla till relevanta nationella aktörer? I åtskilliga strategiska dokument (inte minst kopplade till InfoSäkutredningens arbete) har vikten av internationell och europeisk samverkan inom informationssäkerhetsområdet betonats, men vad detta samarbete specifikt ska innehålla är oklart.

Diskussion och slutsatser: Vår slutsats, baserad på de genomförda intervjuerna, är att svenska aktörer har en stor möjlighet att delta i EU:s arbete inom informationssäkerhetsområdet och även att hämta hem resultat från detta arbete. Sverige borde kunna använda sin befintliga kunskapsbas (inte minst den med koppling till IKT-frågor) och befintliga nätverk och kontaktytor mellan svenska aktörer och deras europeiska motsvarigheter på ett mer strategiskt och koordinerat sätt. Nationell samordning är en viktig fråga i detta sammanhang. Sveriges ständiga representation i EU, lokaliserad till Bryssel, är en viktig resurs.

För ett framgångsrikt agerande på den europeiska arenan krävs både insikt om vad man vill uppnå (påverka riktlinjer, söka forskningsfinansiering, hämta hem information m.m.), hur man ska uppnå detta (delta i seminarier, workshops, komma med ”remissyttranden”, skriva en forskningsansökan etc.) och inte minst vad som krävs (förutsättningar för deltagande, engagemang, alliansbyggande m.m.). Det sistnämnda är särskilt viktigt med tanke på att ersättningsnivån för det nedlagda arbetet inte alltid täcker de faktiska kostnaderna – något som kan vara problematiskt för aktörer utan möjlighet till samfinansiering.

Eftersom Sverige är ett relativt litet land i EU-sammanhang ställs högre

krav för ett framgångsrikt agerande (detta gäller även enskilda aktörer). Förutom ett större deltagande och en hög grad av engagemang krävs också sakkompetens, kunskap om hur EU fungerar och slutligen ”vänner”. Genom att ta reda på hur andra länder ställer sig i enskilt viktiga frågor och hur deras hållning i dessa frågor svarar mot svenska intressen kan man identifiera de aktörer som kan hjälpa till att uppnå en hävstångseffekt inom EU. Det ovanstående är främst skrivet med svenska myndigheter i åtanke, men gäller till stor del också för andra aktörer.

En viktig observation är att det finns ”tidsfönster” när det finns större möjlighet att påverka EU:s handlande i olika frågor. En gynnsam tidpunkt att bidra med underlag till kommissionen är när man inom kommissionen redan arbetar med att ta fram olika relevanta meddelanden. För att lyckas med detta är det viktigt att från svensk sida hålla sig uppdaterad om vilka frågor som kommissionen arbetar med. Ett lämpligt forum för utbyte av information om vad som är på gång inom EU skulle kunna vara KBM:s informationssäkerhetsråd.

För att hämta hem resultaten av EU:s arbete är de främsta verktygen Internet och ett befintligt kontaktnät. Även om de olika aktörernas förmåga att lägga ut relevant information på Internet varierar är Internet ändå den kanske enklaste vägen till information. Där kan man finna såväl utlysningar av forskningsmedel som inbjudan till seminarier och förslag till beslut i olika frågor.

Förslag till vidare studier

Nedan följer ett antal kortfattade förslag till vidare studier som vi under studiens gång har identifierat som intressanta. Sammantaget utgör frågeställningarna – eller kanske snarare svaren på dem – viktiga grundkomponenter i framtagandet av en nationell EU-strategi inom området informationssäkerhet.

Resultat? En studie om lyckade initiativ och förkastade förslag

En processinriktad studie för att närmare analysera resultaten av EU:s arbete inom informationssäkerhetsområdet. Utgångspunkten kan vara ”lyckade initiativ” eller ”förkastade förslag”. Vad är att betrakta som resultat i EU-sammanhang? Finns det ett sätt att definiera lyckade initiativ (exempelvis utifrån antalet direktiv eller förordningar som initiativet resulterat i)? Kan man dra några slutsatser av de förslag som aldrig lett till några konkreta resultat? Finns det frågor som är svåra att adressera i EU-sammanhang? Går det att identifiera tydliga nationella ställningstaganden som kan blockera processen mot ett lyckat initiativ (dvs. frågor kring vilka det i praktiken är omöjligt att enas)?

Den föreslagna studien borde kunna genomföras som en skrivbordsstudie kompletterad med ett antal djupintervjuer av relevanta personer med erfarenhet från EU-arbetet. Resultaten från studien bör kunna utgöra en värdefull grund för hur Sverige kan prioritera EU-arbetet utifrån de förväntade resultaten.

Allierad eller fiende? En studie om att identifiera gemensamma intressen

I denna rapport har vi konstaterat att det för Sverige är viktigt att skapa en förståelse för hur andra länder ställer sig i enskilt viktiga frågor och hur deras hållning i dessa frågor svarar mot de svenska intressena. På så sätt kan man skapa en grund för att identifiera aktörer med vars hjälp det är möjligt att

från svensk sida uppnå en hävstångseffekt inom EU.

Den föreslagna studien syftar till att identifiera och definiera gemensamma intressen bland EU:s medlemsstater inom informationssäkerhetsområdet. En sådan ansats kräver att man tydligt väljer sitt studieobjekt – att utgå från hela informationssäkerhetsområdet är praktiskt ogenomförbart eftersom det skulle kräva för mycket tid och resurser. Därför blir den första uppgiften att definiera utgångspunkten för studien. Enligt ett förslag ska studien baseras på en kvalitativ ansats med djupintervjuer av såväl svenskar verksamma i EU (med god insyn i hur andra länder förhandlar och vilka frågor som är att betrakta som ”nationella hjärtefrågor”) som företrädare från andra medlemsstater och även deras nationella organisationer (för att få en uppfattning om vilka frågor som är aktuella på hemmaplan just nu).

Resultaten från studien torde fungera som viktiga ingångsvärden i allt arbete för att förändra den nuvarande ordningen inom EU när det gäller informationssäkerhetsrelaterade frågor, men de bör även vara intressanta ur ett internationellt perspektiv.

Att välja väg eller hur kan en liten aktör påverka internationellt?

Det är en viktig men svår uppgift att som litet land göra sin röst hörd och påverka utvecklingen på europeisk eller internationell nivå i linje med de svenska intressena. Som tidigare påtalats krävs det ofta mer av en mindre aktör, för ”störst går (oftast) först”. Att välja väg, eller annorlunda uttryckt, att bestämma sig för en gångbar strategi i det internationella arbetet blir således viktigt.

Det finns olika sätt att skapa förutsättningar för ett framgångsrikt agerande utanför Sveriges gränser. Ett sätt är att företräda de svenska intressena (vilka behöver definieras inom informationssäkerhetsområdet) inom EU. Ett annat kan vara att föra samtal med andra nationer som har gjort liknande prioriteringar. Ett tredje sätt skulle kunna vara att lyfta viktiga frågor på en internationell nivå – inte minst eftersom många av frågorna kopplade till informationssäkerhetsområdet är internationella till sin karaktär – exempelvis inom FN.

Den föreslagna studien syftar till att utreda möjligheterna av att framgångsrikt uppnå nationellt identifierade mål i olika kontexter. Finns det några generella slutsatser att dra? Är framgång alltid beroende av frågan eller finns det allmänna förutsättningar som kan identifieras och användas?

Studien föreslås innehålla både skrivbordsmoment och traditionell forskning, och mer scenariobaserade och explorativa delar.[101]

EU:s interna informationssäkerhetsarbete påverkar Sverige

Inom EU pågår ett arbete för att stärka unionens interna informationssäkerhet. Detta arbete hänger delvis samman med att viktiga projekt inom EU ställer ökade krav på just informationssäkerhet. Eftersom detta i sin tur medför konsekvenser för medlemsstaterna, i termer av anpassning m.m., bör det vara intressant att närmare studera EU:s interna informationssäkerhetsarbete – vilka faktorer som driver arbetet och vilka konsekvenser detta får för Sverige. Observera att det är inte bara EU-interna projekt och aktörer som driver EU:s arbete på informationssäkerhetsområdet. Aktörer som exempelvis NATO är också inflytelserika.

Den föreslagna studien kan gärna bedrivas som en skrivbordsstudie kombinerad med ett antal djupintervjuer med representanter från EU:s interna informationssäkerhetsfunktioner.

Att mäta nyttan med EU:s arbete – en fallstudie

Som tidigare påpekats utmynnar EU:s arbete i olika resultat, som t.ex. skapandet av nya organisatoriska enheter. Enisa kan ses som ett sådant direkt resultat av EU:s verksamhet. Den föreslagna studien ska studera nyttan av skapandet av Enisa för de tänkta målgrupperna (här kan de betraktas som ”slutanvändare”). Hur upplever de nyttan av Enisas arbete? Har Enisas arbete haft något genomslag på deras respektive verksamhet och i så fall vilket?

Studien, som till sin karaktär är effektbaserad, föreslås drivas som en fallstudie. Huvudsakligen kvalitativ metodik – djupintervjuer och gruppdiskussioner – kommer att utgöra grundansatsen. I den mån det är möjligt kan man också dra lärdomar från liknande studier, vilket förutsätter en genomgång av den relevanta forskningen på området.

101. En liknande ansats men med annat innehåll redovisas i Maria Oredssons och Mike Winnerstigs rapport (2005): ”Europeisk autonomi eller atlantisk integration? Dagens strukturer och framtida utvecklingslinjer inom ESFP och NATO”. FOI-R 1564 SE.

Sverige en strategisk aktör på EU-arenan – hur?

I denna rapport har vi konstaterat att Sverige har en utmärkt position för att medverka och påverka på den europeiska nivån, men att denna position inte utnyttjas på ett strategiskt sätt. Möjliga orsaker kan bl.a. vara bristande nationell samverkan och avsaknaden av en nationell strategi på området. Vad krävs för att Sverige ska bli en strategisk aktör på den europeiska arenan? Stämmer de orsaksförklaringar som ges i rapporten? Vad kan göras för att vända den nuvarande situationen till en fördel för Sverige? Hur tillvaratas de nationella intressena på ett fruktbart sätt?

Den föreslagna studien kan ta sin utgångspunkt i dagens nationella läge (den svenska intervjuserie som projektet genomfört kan ses som en delmängd av denna ansats) – vilka kontaktytor finns gentemot EU? Detta kan sedan övergå i en diskussion om och analys av hur vi som en nation kan bli bättre på att bl.a. organisera oss för att nå en mer strategisk verkan. Vilka komponenter kan identifieras som viktiga i en nationell strategi?

Referenser

Litteratur

Eriksson, P., och Barck-Holst, S., (2005): ”Politik för skydd av kritisk infrastruktur i EU och i Sverige – en jämförande analys”, [FOI-R—1793—SE]

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

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

Fylkner, M. och Barck-Holst, S. (2005), ”En studie om informationssäkerhet i EU – En precisering av studiens syfte, metod och material”, [FOI Memo 1614]

Oredsson, M. och Winnerstig, M. (2005): ”Europeisk autonomi eller atlantisk integration? Dagens strukturer och framtida utvecklingslinjer inom ESFP och NATO”, [FOI-R—1564-SE]

SIS, (2003), ”Teknisk rapport, handbok 550: Terminologi för informationssäkerhet”

EU-dokument

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

”97/66/EG om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet”

KOM 1998/0395, slutlig: *”Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska centralbanken och Ekonomiska och sociala kommittén – En ram för åtgärder för att bekämpa bedrägeri och förfalskning som rör andra betalningsmedel än kontanter.”*

2000/375/RIF: *”Rådets beslut av den 29 maj 2000 om bekämpning av barnpornografi på Internet”*

KOM 2000/890 slutlig: *”Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén: Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet”*

KOM 2000/0298 slutlig: *”Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – Nät- och informationssäkerhet: förslag till en europeisk strategi”*

Konventionen om Internetrelaterad brottslighet, 2001-11-23

2001/45/EG: *”Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter”*

2001/264/EG: *”Rådets beslut av den 19 mars 2001 om antagande av rådets säkerhetsbestämmelser”*

KOM/2002/0173: *”Förslag till rådets rambeslut om angrepp mot informationssystem”*

2002/475/RIF: *”Rådets rambeslut av den 13 juni 2002 om bekämpandet av terrorism”*

2002/58/EG: *”Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)”*

KOM 2002/0263: *”Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – eEurope 2005: Ett informationssamhälle för alla – En handlingsplan inför Europeiska rådet i Sevilla, den 21–22 juni 2002”*

Ett säkrare Europa i en bättre värld – en europeisk säkerhetsstrategi, 12 december 2003

SEC 2004/332: *”Commission Staff Working Paper. European Security Strategy. The fight against terrorism.”*

SEC 2004/1390: *”Commission staff working document: Consumer Confidence in E-commerce: lessons learned from the e-confidence initiative”*

KOM 2004/702: *”Meddelande från kommissionen till rådet och Europaparlamentet – Skydd av viktig infrastruktur i kampen mot terrorismen”*

KOM 2004/91 slutlig: *”Förslag till Europaparlamentets och rådets beslut om inrättandet av ett flerårigt gemenskapsprogram för att främja en säkrare användning av Internet och ny onlineteknik”*

KOM 2004/0028: *”Meddelande från kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om icke begärd kommersiell kommunikation eller så kallad skräppost”*

2004/55/EG: *”Europaparlamentet och rådets beslut av den 22 december 2003 om utnämning av den oberoende övervakningsmyndighet som föreskrivs i artikel 286 i EG-fördraget (Europeiska datatillsynsmannen)”*

2004/460/EG: *”Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet”*

KOM 2005/121 *”Förslag till Europaparlamentets och rådets beslut om upprättande av ett ramprogram för konkurrenskraft och innovation (2007-2013)”*

KOM 2005/229, slutlig: *”Meddelande från kommissionen till rådet, Europaparlamentet, Europeiska och sociala kommittén samt Regionkommittén – i2010 Det europeiska informationssamhället för tillväxt och säkerhet”*

KOM/2005/0576: *”Grönbok om ett europeiskt program för skydd av kritisk infrastruktur”*

2005/752/EG: *”Kommissionens beslut av den 24 oktober 2005 om inrättande av en expertgrupp för elektronisk handel”*

2006/24/EG: *”Europaparlamentets och rådets direktiv av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG”*

KOM 2006/0251, slutlig: *”Meddelande från kommissionen till Rådet, Europaparlamentet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – En strategi för ett säkert informationssamhälle – Dialog, partnerskap och användarinflytande”*

Svenska dokument

SOU 2004:32, *”Informationssäkerhet i Sverige och internationellt – en översikt”,* Delrapport 2 från InfoSäkutredningen

SOU 2005:71, *”Informationssäkerhetspolitik, organisatoriska konsekvenser”,* InfoSäkutredningens slutbetänkande

Proposition 2005/06:133, *”Samverkan i kris – för ett säkrare samhälle”*

Cirkulär med riktlinjer för handläggningen av kommissionens offentliga samråd, Utrikesdepartementet, 2004-06-08

Övrigt material (webbresurser)

Europeiskt centrum för förebyggande och kontroll av sjukdomar (ECDC) http://europa.eu/agencies/community_agencies/ecdc/index_sv.htm 200606-21

Information Society Technologies http://cordis.europa.eu/ist 2006-06-28

Budget breakdown of the Seventh Framework Programme of the European Community http://cordis.europa.eu/fp7/breakdown.htm 2006-06-28

Generaldirektoratet för energi och transport – Generaldirektörens uppdrag http://ec.europa.eu/dgs/energy_transport/matthias_ruete/mission_sv.html 2006-05-22

Security in transport and energy http://ec.europa.eu/dgs/energy_transport/security/infrastructure/index_en.htm 2006-05-22

Joint Research Centre www.jrc.ec.europa.eu 2006-05-22

Institute for the Protection and Security of the Citizen http://ipsc.jrc.cec.eu.int/listfp.php?id=7 2006-05-22

EU – Konsumentfrågor http://ec.europa.eu/consumers/index_sv.htm 2006-05-24
EU – Security of Payments http://ec.europa.eu/comm/consumers/cons_int/e-commerce/secur_en.htm 2006-05-24
Regelverk för elektronisk kommunikation http://europa.eu/scadplus/leg/sv/lvb/l24216a.htm 2006-06-30
Unsolicited communications – Fighting Spam http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm 2006-06-15
Socialstyrelsen www.socialstyrelsen.se 2006-06-30
CI2RCO http://www.ci2rco.org 2006-06-30
Members of the Expert Group on electronic commerce http://ec.europa.eu/internal_market/e-commerce/expert-group-members_en.htm 2006-05-24
KOM 2005/121 Om upprättande av ett ramprogram för konkurrenskraft och innovation (2007-2013) http://ec.europa.eu/enterprise/enterprise_policy/cip/docs/com121_sv.pdf 2006-05-30
IDABC Work Programme 2005-2009 http://ec.europa.eu/idabc/en/document/5101/3 2006-05-30
CORDIS – Security Research – Find a document http://cordis.europa.eu/security/findoc.htm 2006-05-30
Introducing – DG JLS – European Commission http://ec.europa.eu/dgs/justice_home/index_en.htm 2006-05-24
Rådsarbetsgrupper för inrikes och rättsliga frågor http://www.regeringen.se/sb/d/6331 2006-02-20
Rådsarbetsgrupper för konkurrensfrågor (EU:s inre marknad, industri och forskning) http://www.regeringen.se/sb/d/2823 2006-02-20
Rådsarbetsgrupper för transport, telekommunikation och energi http://www.regeringen.se/sb/d/6341 2006-03-14
Enisa http://enisa.eu.int 2006-05-30
EU-upplysningen http://www.eu-upplysningen.se 2006-05-31
Europol http://www.europol.eu.int 2006-05-31
Eurojust http://www.eurojust.eu.int 2006-03-30
Institute for Security Studies http://www.iss-eu.org 2006-06-30
List of Chaillot Papers – Institute for Security Studies http://www.iss-eu.org/public/content/chaile.html 2006-05-30
Europeiskt myndighetssamarbete mot spam http://www.rattsinformation.konsumentverket.se/mallar/sv/artikel_datum.asp?lngCategoryId=977&lngArticleId=4644 2006-06-30
Consultation, the European Commission and Civil Society http://ec.europa.eu/civil_society/coneccs/index_en.htm 2006-06-13

EU-upplysningen – Regler för lobbyister i EU http://www.eu-upplysningen.se/templates/EUU/standardRightMenuTemplate____2862.aspx 2006-04-11

KBM:S TEMASERIE

2006:5 Vem gör vad inom EU?
Informationssäkerhetsfrågorna i fokus

2006:4 Terrorattackerna i London
Brittiska lokala och regionala myndigheters agerande
och lärdomar för det svenska krishanteringssystemet

2006:3 Så fungerar författningen vid kriser
En studie av hur statsmakterna hanterat morden på Olof Palme och Anna Lindh

2006:2 Privat-offentlig samverkan
Från idé till fungerande praktik

2006:1 Kriskommunikation via webben
Studier av dubbelmordet i Linköping, Kemiraolycka och stormen Gudrun

2005:13 Tsunamins genomslag
En studie av svenska mediers bevakning

2005:12 Fred i det europeiska rummet
Konflikttrender i Europa, Mellanöstern, Afrika och Centralasien 1989–2003

2005:11 Hot- och riskrapport 2005

2005:10 Medborgare om våldsdåd
Reaktioner efter mordet på Anna Lindh och andra dåd

2005:9 Samverkan i organisation eller nätverk?
Fallen elektroniska affärer och elberedskap

2005:8 Mind the gap!
Hur bygger vi broar mellan stat och näringsliv i arbetet med krisberedskap?

2005:7 Hot på agendan
En analys av nyhetsförmedling om risker och kriser

2005:6 Samverkan mellan offentlig sektor och näringslivet vid krishantering
En studie av kriser i Sverige 1993–2003

2005:5 Förtroendekriser
Kommunikationsstrategier före, under och efter

2005:4 Efter flodvågskatastrofen
Svenska folkets åsikter om och förtroende för myndigheter, medier och politiker

2005:3 Propagandakriget i backspegeln
En studie i påverkansförsök och svenska nyhetsmedier

2005:2 Allmänheten medverkar vid övningar
Erfarenheter från Övning Havsörn

2005:1 Beredskap mot skadlig kod
En kartläggning av IT- och informationssäkerheten inom större myndigheter
och statliga bolag i Sverige med fördjupad analys av skadlig kod

Vem gör vad inom EU?

INFORMATIONSSÄKERHETSFRÅGORNA I FOKUS

Vem gör vad inom EU – informationssäkerhetsfrågorna i fokus är en studie som tar upp aktörer, processer och ansvar på europeisk nivån avseende informationssäkerhet. Studien skall ses som ett led i att förbättra möjligheterna för svenska myndigheter att både delta i och påverka informationssäkerhetsarbetet på europeisk nivå.

Förhoppningen är att resultatet av studien skall utgöra en plattform för vidare studier samt ett förbättrat svenskt agerande på området.

Studien riktar sig till läsare som är insatt i frågor som rör informationssäkerhet och som har behov av en guide till EU:s arbete inom området snarare än läsare som är kunniga om EU och vill fördjupa sig i informationssäkerhetsfrågor.

ISSN 1652-2915
ISBN 91-975934-0-0

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se