Politik för skydd av kritisk infrastruktur i EU och Sverige - en jämförande analys

PÄR ERIKSSON, SVANTE BARCK-HOLST

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1350 anställda varav ungefär 950 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Försvarsanalys
164 90 Stockholm

Tel: 08-555 030 00
Fax: 08-555 031 00

www.foi.se

FOI-R--1793--SE
ISSN 1650-1942

Användarrapport
December 2005

Försvarsanalys

Pär Eriksson, Svante Barck-Holst

Politik för skydd av kritisk infrastruktur i EU och Sverige - en jämförande analys

FOI-R--1793--SE
ISSN 1650-1942

Försvarsanalys
Användarrapport

December 2005

Omslagsbild: Microsoft Clipart

Utgivare	Rapportnummer, ISRN	Klassificering
FOI - Totalförsvarets forskningsinstitut Försvarsanalys 164 90 Stockholm	FOI-R--1793--SE	Användarrapport
	Forskningsområde 1. Analys av säkerhet och sårbarhet	
	Månad, år December 2005	**Projektnummer** E1919
	Delområde 13 Stöd till säkerhet och beredskap	
	Delområde 2	

Författare/redaktör	Projektledare
Pär Eriksson Svante Barck-Holst	Helén Jarlsvik
	Godkänd av Staffan Molin
	Uppdragsgivare/kundbeteckning Krisberedskapsmyndigheten
	Tekniskt och/eller vetenskapligt ansvarig Karin Mossberg Sonnek

Rapportens titel

Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys

Sammanfattning

Efter terrordåden i Madrid 2004 har diskussionen tagit fart om en sektorsövergripande roll för EU avseende skydd av kritisk infrastruktur. Denna studie jämför de i EU diskuterade förslagen med svensk politik. En central del av rapporten är formulerandet av tentativa jämförelsefaktorer.

Vid en analys av tillgängliga dokument framtonar två alternativa roller för EU i ett eventuellt framtida sektors-övergripande CIP-system: Dels ett Kommissionskontrollerat, centraliserat system med en uppifrån och ned-process för att identifiera, analysera och skydda kritisk infrastruktur, dels ett decentraliserat system där EU:s roll är att främja en ökad grad av samsyn, koordination och samverkan men där kontroll ligger kvar hos medlemsstaterna.

I rapporten konstateras att det ur ett svenskt perspektiv finns, inte minst utifrån ökad transnationalisering och multinationalisering av kritisk infrastruktur, skäl att bejaka en ökad EU-roll. Ett EU-system, framförallt då ett mer styrande, får emellertid konsekvenser för det svenska krisberedskapssystemet som bygger på ett nedifrån och upp system med självständiga sakområdesmyndigheter. Därför behöver en rad frågor rörande svensk myndighetsstruktur, avgränsningen mellan vad som skall vara nationell respektive europeisk kritisk infrastruktur samt hur svenska krisberedskapsprioriteringar skulle påverkas av ett europeiskt system analyseras vidare i närtid.

Nyckelord

Skydd av kritisk infrastruktur, EU, KBM, Sverige

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 89 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization FOI – Swedish Defence Research Agency Försvarsanalys 164 90 Stockholm	**Report number, ISRN** FOI-R--1793--SE	**Report type** User report
	Programme Areas 1. Security, safety and vulnerability analyses	
	Month year December 2005	**Project no.** E1919
	Subcategories 13 Support to Security, Safety and Preparedness	
	Subcategories 2	

Author/s (editor/s) Pär Eriksson Svante Barck-Holst	**Project manager** Helén Jarlsvik
	Approved by Staffan Molin
	Sponsoring agency Swedish Emergency Management Agency
	Scientifically and technically responsible Karin Mossberg Sonnek

Report title (In translation)

Critical Infrastructure Protection Policy in the EU and in Sweden - a comparative analysis

Abstract

After the terrorist attack in Madrid 2004, the discussion on the possible future role for the EU regarding critical infrastructure protection (CIP) gained momentum. This study compares the proposals discussed within the EU with Swedish policy. An important part of the report is the development of tentative, comparative factors.

Two alternative, possible future roles for the EU regarding CIP can be discerned from the EU documents: Either a system controlled by the Commission, quite centralised and with a top down process to identify, analyse and protect critical infrastructure, or a decentralised system where the role of the EU rather is to encourage and support the development of common views, coordination and cooperation but where the control remains with the Member States.

In this report it is noted that from a Swedish perspective, not least due to the increased trans-nationalisation and multi-nationalisation of critical infrastructures, an enhanced role for the EU would have advantages. However, an EU system, especially a more centralised one, will also have consequences for the Swedish system, which is based on a bottom-up approach with independent agencies. Hence there is a number of questions that have to be analysed urgently, for instance concerning the Swedish structure of agencies, the delineation between what should be defined as national and European infrastructure and how Swedish CIP-priorities could be affected by an EU critical infrastructure protection policy.

Keywords

Critical Infrastructure Protection, EU, SEMA, Sweden

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 89 p.
	Price acc. to pricelist

Innhållsförteckning

Förord

EU har länge arbetat med frågor som kan hänföras till skydd av kritisk infrastruktur. Det har emellertid skett sektorsvis – flygsäkerhet, livsmedelssäkerhet, informationssäkerhet etc. Först efter terrordåden i Madrid 2004 har diskussionen om behovet av en sektorsövergripande EU-politik avseende skydd av kritisk infrastruktur tagit fart på allvar.

I oktober 2004 presenterade Kommissionen ett meddelande där riktlinjerna för ett tämligen långtgående europeiskt program för skydd av kritisk infrastruktur lades fast. Detta följdes upp under 2005 med en process av flera seminarier och ett grönpapper om skydd av kritisk infrastruktur. Målet är att lägga fast en politik för EU:s arbete med kritisk infrastruktur under 2006. Den riktning som Kommissionen önskar gå mot är emellertid inte oomstridd och såväl inom EU:s institutioner som bland medlemsstaterna finns det de som vill se ett mindre långtgående europeisk system för skydd av kritisk infrastruktur.

Det är mot bakgrund av denna utveckling som FOI fick i uppdrag av Krisberedskapsmyndigheten (KBM) att genomföra en kortare studie i syfte att studera hur svensk och europeisk politik rörande kritisk infrastruktur förhåller sig till varandra. Här föreliggande rapport är en redovisning av detta arbete.

Rapporten har granskats av Henrik Christiansson, FOI:s avdelningen för Försvarsanalys. Vi vill tacka honom för värdefulla synpunkter och diskussioner. Vi vill också tacka Krisberedskapsmyndigheten för givande diskussioner vid två arbetsseminarier under studiens gång. Studiens eventuella brister och felaktigheter är dock helt författarnas ansvar.

Rapporten är en av flera rapporter som har skrivits vid FOI under de senaste åren inom kompetensområdet Euroatlantisk säkerhet. Kompetensområdet består av ett femtontal forskare som arbetar med olika aspekter av europeiska och transatlantiska frågeställningar – civil och militär krishantering, inre och yttre säkerhet, EU och Nato – på uppdrag av svenska departement och myndigheter. Kunskapsuppbyggande studier varvas med mer policynära analyser och direktstöd. Ett centralt tema för arbetet inom kompetensområdet är kopplingen mellan den internationella och nationella nivån.

Helén Jarlsvik,
Projektledare

Pär Eriksson,
Huvudförfattare

0 Sammanfattning

0.1 Bakgrund, syfte och metod

EU har beslutat att utveckla en sektorsövergripande politik avseende skydd av kritisk infrastruktur (på engelska ”Critical Infrastructure Protection” eller ”CIP”). Redan tidigare har EU i specifika sakpolitikområden, som t.ex. livsmedelssäkerhet och skydd mot kemolyckor, haft en politik med inslag av CIP-aspekter. Efter terrordåden 2001 och framåt har emellertid behovet av och trycket för att EU skall ha en också sektorsövergripande roll ökat, inte minst på grund av infrastrukturernas allt större beroende av varandra. Med tiden har diskussionen kommit att handla om ett bredare hotspektrum än bara terrorism.

Denna studie syftar till att göra en jämförelse mellan de inom EU diskuterade formerna för en sektorsövergripande CIP-politik och det svenska systemet. Det stod tidigt i arbetet klart att det fanns mycket lite av forskning att falla tillbaka på när det gällde detta slags jämförelser på systemnivå varför en del av studien blev att identifiera ett antal tentativa, relevanta och sektorsövergripande jämförelsefaktorer. Utgångspunkten för denna identifiering utgörs av en nedbrytning av CIP-begreppet, kompletterat med de frågeställningar som de få komparativa studierna betonar samt den empiri som finns i form av diskussioner som förts i olika internationella sammanhang.

Studien omfattning har emellertid inte tillåtit att analysera dessa faktorer i detalj. Att fortsätta att utveckla jämförelsefaktorerna för att på så vis finna en modell för att jämföra olika systems för- och nackdelar är ett område för fortsatt forskning, inte minst mot ljuset av EU-processens strävan att i allt högre grad närma medlemsstaternas system till varandra.

De jämförelsefaktorer som utnyttjas är:

- Vad utgör kritisk infrastruktur?
    - Vad utgör kritisk infrastruktur?
    - Vad utgör transnationell kritisk infrastruktur?
    - Hur identifieras kritisk infrastruktur och av vem?
- Mot vad skall kritisk infrastruktur skyddas?
    - Vad betraktas som relevanta hot?
    - Hur definieras hotet och av vem?
- Hur skall skyddet utformas?
    - Vilken/vilka faser i skyddsarbetet lägger man tonvikten på?

- Vilken karaktär skall multinationella åtgärder för skydd av kritisk infrastruktur få?
- Vem ansvarar för skyddet av kritisk infrastruktur?
- Hur finansieras skydd av kritisk infrastruktur?

EU:s sektorsövergripande politik för CIP befinner sig fortfarande på diskussionsstadiet. Därför behöver såväl den övergripande politiska nivån av strategier och program som den CIP-specifika nivån av diskussioner och dokument rörande en framtida, sektorsövergripande europeisk CIP-politik ligga till grund för analysen. Vidare genomförs redan idag CIP-relaterade åtgärder i specifika politikområden varför även dessa utgör ett ingångsvärde för analysen.

0.2 Två bilder av EU:s framtida politik för skydd av kritisk infrastruktur

Vid en analys av EU:s framtida, potentiella roll inom skydd av kritisk infrastruktur framtonar två olika bilder: Den första bilden, som framförallt återfinns i Kommissionsdokument, är den av ett Kommissionskontrollerat, centraliserat system med en uppifrån och ned-process för att identifiera, analysera och skydda kritisk infrastruktur.

I detta förutses ett gemensamt ramverk av kriterier och processer inom vilket EU tillsammans med medlemsstaterna ansvarar för europeisk kritisk infrastruktur och medlemsstaterna, med utgångspunkt från ramverket, ansvarar för nationell kritisk infrastruktur. I diskussionerna ingår också införandet av nationella myndigheter ansvariga för att driva det europeiska programmet för skydd av kritisk infrastruktur och register på nationell och europeisk nivå över nationell respektive europeisk kritisk infrastruktur.

Den andra bilden, som framförallt återfinns i de program och strategier som Rådet beslutat (Haagprogrammet, Handlingsplanen för terrorismbekämpning, Solidaritetsprogrammet etc.), är den av ett decentraliserat system där EU:s roll är att befrämja en ökad grad av samsyn, koordination och samverkan när det gäller skyddet av kritisk infrastruktur men där den konkreta kontrollen över CIP ligger kvar hos medlemsstaterna. Utbyte av kunskap om metoder för analys av hot, risker och sårbarheter liksom erfarenheter bl.a. i form av best practices för skydd utgör kärnpunkter.

Bägge dessa roller innebär att EU påverkar såväl horisontella, sektorsövergripande aspekter som vertikala sektorsspecifika aspekter av CIP. Även i ett decentraliserat system skulle det kunna bli aktuellt med att införa nya instrument till stöd för en europeisk CIP-politik.

0.3 Sverige och en EU-politik för skydd av kritisk infrastruktur

Sverige har ett i huvudsak decentraliserat krisberedskapssystem, med en planeringsprocess präglad av ”nedifrån och upp” och förhandling inom och mellan samverkansområden för att finna prioriteringar och fördela medel. Det uppstår betydande utmaningar när man skall jämka samman detta med de slags system som nu diskuteras på den europeiska nivån. Mest komplicerat skulle det bli avseende ett mer styrande, uppifrån och ned system liknande det som Kommissionen förespråkar. Några av de viktigaste utmaningarna utgörs av:

- **Svenska myndighetsstrukturen**. Det svenska systemet bygger på sakmyndigheter med betydande ansvar och en sektorsövergripande myndighet, Krisberedskapsmyndigheten, med en samordnande och processdrivande – inte styrande – roll. Ett europeiskt, sektorsövergripande system skulle väcka ett antal frågor. Vilken myndighet skall representera Sverige i utvecklingen och vidmakthållandet av ett sådant system? Vilka myndigheter skall delta i implementeringen av detta system? Hur skall sektorsövergripande analyser och direktiv föras in i det svenska systemet utan att sakmyndigheterna blir marginaliserade?

- **Svenska kontra europeiska prioriteringar**. Den för EU föreslagna processen för identifiering och analys av kritisk infrastruktur, grundad i tydliga definitioner, kan leda till andra prioriteringar när det gäller vilka konkreta infrastrukturer som skall skyddas än den förhandlingsbaserade process Sverige för närvarande grundar sin planering på. EU:s arbete med CIP ingår inte heller på samma sätt i en helhet av krisberedskapstänkande, utan är mer av ”stand alone”. Därmed finns det risk för att svenska prioriteringar kan komma att påverkas av EU-politiken. Det gäller t.ex. den svenska prioriteringen av krishanteringsförmåga framför skydd av specifika kritiska infrastrukturer med motivet att det inte går att skydda allt men att samhället alltid måste kunna hantera en kris som uppstår. En ytterligare aspekt rörande prioriteringar rör hur pass styrande och normerande en gemensam europeisk hotbild skall vara – gemensamma diskussioner om hot och hotbild kan vara ett medel att öka den gemensamma förståelsen och kunskapen om hotet men kan samtidigt också likrikta åtgärder över hela EU på ett sätt som inte är relevant, t.ex. på grund av olika geografiska, klimatologiska eller geografiska förhållanden.

- **Avgränsning mellan nationell och transnationell kritisk infrastruktur**. Vad som pekas ut som kritisk infrastruktur och särskilt vad som pekas ut om europeisk kritisk infrastruktur blir en avgörande faktor för räckvidden för EU:s inflytande över CIP. Kriterierna för att avgöra dessa avgränsningar är emellertid inte klara. Det är samtidigt också oklart vilken

roll EU mer konkret skall ha relativt europeisk respektive nationell infrastruktur. Med nationella CIP-myndigheter ansvariga för att genomföra EU-politiken nationellt – och då också rörande nationell infrastruktur inom ett ”gemensamt ramverk” – kan det nationella rörelseutrymmet minska betydligt.

- **Relationen till ägare/operatörer**. I Sverige förs idag dialogen med ägare/operatörer till allra största del genom sakansvariga myndigheter. Med ett europeiskt system med CIP-inriktade branschorganisationer på Unionsnivå, kan kontakterna med ägare/operatörer bli mer centraliserade. Huruvida relationen mellan det allmänna (EU och medlemsstater) och ägare/operatörer skall vara lagtvingad, frivillig eller någonstans mittemellan är också en fråga där det kan finnas olika syn hos Sverige, andra medlemsstater och EU. Naturen hos EU:s diskuterade förslag för ett europeiskt program för skydd av kritisk infrastruktur är centralstyrt med miniminormer vilket kan innebära ett i grunden mer lagstyrt förhållningssätt till ägare/operatörer än vad Sverige för tillfället har. Detta kan i sin tur också innebära att den svenska myndighet som eventuellt utses till CIP-myndighet skulle behöva ha mer av direktkontakter med ägare/operatörer, åtminstone vad gäller sektorsövergripande, horisontella frågor, än vad som är aktuellt för KBM i dagens system.

- **Finansieringsformer**. Sverige och EU har bägge som huvudprincip att ägare/operatörer ansvarar för skyddet av de egna anläggningarna. Emellertid påpekar Kommissionen att när det gäller hot mot samhället som helhet måste också samhället vara berett att ta på sig ett ansvar för kostnader för skyddet. På EU-nivån finns ännu inte någon diskussion om var gränsen går mellan, för att använda svensk terminologi, grundsäkerhet och förstärkt förmåga, varför frågan om vilka delar som i ett EU-system kan komma att ses som i behov av en finansiering från det allmänna är svår att besvara. Det är inte heller säkert att medlemsstaterna har en gemensam syn avseende vilka finansieringsformer (skattefinansiering, avgiftsfinansiering, frivillig egenfinansiering, lagstyrd egenfinansiering) som är lämpliga för olika sektorer, t.ex. på grund av olika grad av avreglering. Här kan en harmonisering komma att påverka tidigare svenska ställningstaganden.

Flera av dessa utmaningar blir lättare att hantera om EU skulle gå mot ett system med en roll att främst stödja samordning och informationsutbyte. Emellertid syftar även ett sådant system till ett tillnärmande mellan de nationella regelverken över tiden varför utmaningarna i de flesta fall ändå kommer att aktualiseras med tiden.

En europeisk, sektorsövergripande politik för CIP torde också vara ett svenskt intresse. Med den internationalisering och multinationalisering som skett av kritisk infrastruktur de senaste decennierna är även Sverige en del av ett internationellt sammanhang och beroende av infrastrukturer utanför nationell kontroll. En kärnfråga är därför avvägningen mellan detta intresse av ökat samarbete och priset i form av att överlämna inflytande och befogenheter till EU.

EU:s framtida politik för skydd av kritisk infrastruktur är fortfarande vag i konturerna. De stora medlemsstaterna, som inte varit i fokus för denna studie, kan komma få ett stort inflytande på den slutliga utformningen. Olika stater kan också vilja se olika principer en sektorsövergripande CIP-politik men också olika prioriteringar i frågor som vilka skyddsinsatser som skall prioriteras och vilka resurser, t.ex. för återställande av infrastruktur, som skulle kunna bli aktuella att samordnas av EU.

Samtidigt innebär osäkerheten att det finns ett utrymme för ett proaktivt svenskt agerande för att påverka den slutliga utformningen av EU:s CIP-politik. I ett sådant agerande ingår såväl att lägga offensiva förslag som att bygga allianser med andra likasinnade medlemsstater. Det kräver emellertid att Sverige skaffar sig en tydlig bild av vad man anser vara nödvändigt och önskvärt att uppnå med en EU-roll. Utifrån svaren på dessa frågor kan sedan en svensk linje formuleras avseende konkreta sakfrågor som kriterier för att identifiera kritisk infrastruktur, hur processen för att identifiera och analysera infrastruktur skall se ut, finansieringsformer etc.

1 Inledning

1.1 Bakgrund

De senaste årens terrordåd, inte minst de i USA 2001, Madrid 2004 och London 2005, har inneburit att väst betraktar omvärlden genom delvis nya glasögon. Uppfattningen om dominerande hot har förskjutits, kartan över allierade och motståndare har ritats om och kraven på mer långtgående åtgärder mot terrorism har ökat.[1] Den förändrade synen på terrorism har vidare inneburit att det blivit allt svårare att i den europeiska debatten hävda den tidigare så skarpa skiljelinjen mellan ”traditionellt” försvar mot externa fiender och intern krishantering t.ex. för att hantera terrorism.[2] På så vis blir skyddet av kritisk infrastruktur en central del i samhällets robusthet även gentemot dagens externa hot.

Synen på skydd av kritisk infrastruktur har också förändrats. Under det kalla kriget var skydd av kritisk infrastruktur främst inriktat på att möta ett storskaligt angrepp från en extern fiende. Idag handlar det om att kunna skydda samhällets infrastruktur från ett mycket bredare spektrum av hot samtidigt som acceptansen för t.ex. ett tele- eller elavbrott har minskat. Även mindre störningar måste kunna förutses och förhindras. Händelser som stormen Gudrun i Sverige januari 2005 och de stora översvämningarna i olika delar av Europa under de senaste åren har samtidigt visat att fokus inte enbart får ligga på aktörsinducerade händelser. Även naturhändelser kan få omfattande påverkan på ett modernt samhälle och dess infrastrukturer.[3]

Parallellt har beroendet över nationsgränserna ökat när det gäller kritisk infrastruktur. Europas stater är numera sammanbundna av gemensamma, i vissa fall globala, infrastrukturssystem. Därmed delar de i allt högre grad såväl sårbarheter som hotbild med varandra och med sin omvärld. De nationella systemen är beroende av varandra och om ett system slutar att fungera i en medlemsstat kan det få effekter i andra.

Oavsett om det handlar om aktörsstyrda eller aktörsoberoende hot finns det således behov av olika former av skydd av europeisk infrastruktur i vid bemärkelse. Det kan handla om förebyggande, avvärjande och/eller återställande insatser. Inom enskilda, specifika politikområden, som t.ex. flygsäkerhet, har det också under en längre tid funnits åtgärder på EU-nivån som kan ses som skydd av infrastruktur. Utvecklingen de senaste åren har emellertid inneburit ett ökat

[1] Se t.ex. Pär Eriksson: ”Konsekvenser för EU, ESDP och Sverige”, i Bo Ljung (ed.): *Uppföljningsstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser*, FOI-R--0471--SE, april 2002.
[2] Se vidare Pär Eriksson “EU:s säkerhets- och försvarspolitik” i Gunilla Derefeldt, Henrik Friman (red.): *Samhällsförsvar – nya hot och ökat internationellt engagemang*, Conference Papers 32, Utrikespolitiska Institutet, Stockholm 2004.
[3] Utanför Europa är orkanen Katrinas härjningar det kanske allra tydligaste exemplet.

tryck även för ett större gemensamt, sektorsövergripande ansvar för skydd av kritiska infrastrukturer (Critical Infrastructure Protection, CIP). Efter bombdåden i Madrid inleddes också arbetet att utveckla en sektorsövergripande europeisk CIP-politik. Bland annat initierades en process för att ta fram ett europeiskt program för CIP, EPCIP.

Den pågående processen att utveckla en europeisk politik avseende skydd av kritisk infrastruktur kommer att påverka det svenska krisberedskapssystemet. Därför är det av vikt att inte bara beskriva det framväxande europeiska systemet utan även att diskutera hur detta förhåller sig till det svenska, nationella systemet. En sådan diskussion utgör en grund för att avgöra om och hur Sverige bör agera på en EU-nivå för att påverka EU:s politik men också om och hur Sverige kan behöva förändra sitt eget nationella system för att bättre anpassa detta till EU.

1.2 Syfte och avgränsningar

Syftet med denna studie är att studera hur svensk och europeisk politik rörande kritisk infrastruktur förhåller sig till varandra. Mer specifikt syftar studien till att med hjälp av ett antal för området skydd av kritisk infrastruktur relevanta, och i sin karaktär sektorsövergripande, faktorer jämföra Sveriges arbete med skydd av kritisk infrastruktur med det framväxande EU-samarbetet inom samma område. Dessutom diskuteras ett antal tentativa konsekvenser av eventuella skillnader. Ett centralt delmoment i studien är att identifiera och definiera jämförelsefaktorerna.

Målet är att studiens slutsatser skall kunna utnyttjas i överväganden kring när ett aktivt svenskt agerande på EU-nivån är påkallat eller när ett svenskt förändringsarbete på den nationella nivån krävs för att hantera utvecklingen på EU-nivån.

En central avgränsning för studien är att uppdraget är att jämföra EU:s framväxande politik för skydd av kritisk infrastruktur, såsom den utryckes i dokument och beslut, med svensk politik för skydd av kritisk infrastruktur. Det kan argumenteras att det vore minst lika viktigt att göra en jämförelse mellan de dominerande medlemsstaterna och Sverige, då EU i många avseende utgör summan av sina medlemsstater. Detta har dock inte varit möjligt inom denna studies ram. Här kan bara noteras att denna avgränsning innebär att medlemsstaternas roll delvis hamnar i skymundan medan de i verkligheten kan komma att få ett stort inflytande på vad som är möjlig och önskvärd CIP-utveckling

inom EU. Medlemsstaternas syn utgör således ett viktigt ingångsvärde för den svenska analysen av EU:s framtida CIP-politik.[4]

Det pågår redan idag CIP-samarbete inom Europa som EU inte är involverat i, bilateralt eller multilateralt. Dessutom arbetar ägare/operatörer med att skydda sin infrastruktur. Erfarenheterna av detta sektorsspecifika arbete utanför EU-ramen kan också komma att bli ett viktigt ingångsvärde i skapandet av en EU-politik för CIP. Det har emellertid inte inom denna studies begränsade ram varit möjligt att göra en analys av dessa samarbeten.

Begreppet ”skydd av kritisk infrastruktur” är vagt och definieras olika i olika sammanhang. Därför utgår denna studie från en vid tolkning. Emellertid uppstår ändå tidvis vissa avgränsningsproblem. Skall t.ex. konsekvenshantering ses som en del av CIP? Detta blir särskilt besvärligt då förmågan att återställa kritisk infrastruktur som slagits ut eller skadats många gånger flyter samman med konsekvenshanteringen. I arbetet har emellertid konsekvenshantering generellt sett inte ansetts som en del av skyddet av kritisk infrastruktur. Detta ligger i linje med såväl svensk som europeisk grundsyn.

En ytterligare avgränsning är att även om CIP studeras i en tämligen vid bemärkelse berörs bara undantagsvis EU:s lagstiftningsarbete visavi terrorism. Det kan argumenteras att med en vid definition av CIP borde även detta tas med i analysen. Tids- och omfångsmässigt har detta dock inte bedömts som görligt samtidigt som det bara skulle vara av mindre intresse för denna rapport.

Slutligen används termen ”skydd av kritisk infrastruktur” och den internationellt vedertagna förkortningen ”CIP” som synonymer i texten.

1.3 Forskningsläget

En genomgång av tillgänglig forskning visar att det är svårt att finna arbeten som studerar sektorsövergripande system för skydd av kritisk infrastruktur på nationell eller övernationell nivå, eller hur ett bra nationellt eller internationellt sådant system bör vara utformat. Till del kan det ha att göra med att staters tradition och arv så starkt styr hur man arbetar med skydd av kritisk infrastruktur varför jämförande studier blir svåra. Ett ytterligare tänkbart skäl kan vara att bakom de existerande systemen ligger politiska beslut och att det därför inte finns något intresse för att finansiera forskning som möjligen skulle visa att dessa beslut inte lett till optimala strukturer. Slutligen kan ett skäl också vara att forskare engagerade i CIP-relaterad forskning i allmänhet är mer intresserade av

[4] I studien diskuteras inte heller kopplingen mellan den CIP-utveckling som skett i USA efter den 11 september och den utveckling som sker i EU och dess medlemsstater. Även detta samband har relevans för vad som till syvende och sidst kommer att vara möjligt, nödvändigt och önskvärt inom EU-ramen avseende CIP.

specifika sakområden, som t.ex. risk- och sårbarhetsanalyser, än av övergripande policyrelaterade systemfrågor.

Det finns således mycket lite av forskning kring möjliga modeller för uppbyggnaden av nationella eller övernationella system och arrangemang för skydd av kritisk infrastruktur. De studier som har gjorts är istället ofta studier genomförda av statliga myndigheter och organ.[5] Däremot finansieras en mängd forskning i Sverige, i EU och globalt när det gäller olika delområden av systemet, bl.a. riskidentifiering, risk- och sårbarhetsanalys, privat-offentlig samverkan, infrastruktursäkring och beroenden.[6] Det finns också betydande mängd fallstudier, allt från mer beskrivande analyser till analyser där fallstudier utnyttjas för att dra slutsatser av en mer principiellt generell natur, t.ex. rörande ”best practices”.[7]

Ett av relativt få undantag när det gäller övergripande, jämförande CIP-studier utgörs av ”International CIIP Handbook 2004”, utgiven av Swiss Federal Institute of Technology i Zürich. I denna redovisas ett antal länders arbete med skydd av kritisk infrastruktur i allmänhet och skydd av informationsinfrastrukturen (CIIP) i synnerhet, på ett jämförbart sätt. Boken innehåller dessutom flera avsnitt i vilka man just jämför olika staters politik rörande olika CIP/CIIP-relaterade frågor.[8]

Eftersom CIP-frågor kommit upp på EU-agendan först de senaste åren finns det relativt lite material, utöver officiella dokument, om EU:s arbete med skydd av kritisk infrastruktur. Det som finns riskerar dessutom att bli inaktuellt tämligen snabbt då området är under snabb utveckling. Här torde emellertid i framtiden finnas ett behov av fördjupad forskning, inte minst kring diskussionen om vilket mervärde en övernationell nivå som EU kan tillföra CIP-arbetet.

1.4 Metod och material

För att uppnå studiens syfte att jämföra EU:s framväxande politik för skydd av kritisk infrastruktur med den svenska modellen behöver ett antal sektorsövergripande, för CIP-området relevanta, jämförelsefaktorer identifieras och definieras. En hypotes i det förberedande arbetet med studien var att kunna utnyttja redan genomförd forskning av övergripande CIP-system för att identifiera dessa faktorer. En fördel med ett sådant angreppssätt vore en ökad grad av helhetssyn

[5] Ett exempel är Krisberedskapsmyndigheten: *Krisberedskap i omvärlden*, KBM:s temaserie, 2003:3.
[6] Se t.ex. Krisberedskapsmyndighetens hemsida (www.krisberedskapsmyndigheten.se) och den forskning som där belyses, EU:s hemsida kring säkerhetsforskning (www.cordis.lu/security/) eller hemsidan för Kanadas nationella säkerhetsforskning (www.psepc.gc.ca). I Sverige är t.ex. forskargruppen LUCRAM en aktör inom denna typ av forskning.
[7] EU:s Joint Research Centre har t.ex. ansvar för att samla in, sammanställa, analysera och sprida kunskap om olyckor rörande farliga ämnen. På en mer generell krishanteringsnivå bedriver i Sverige forskningsgruppen CRISMART på Försvarshögskolan fallstudier. Se vidare CRISMART hemsida, www.crismart.org.
[8] Andreas Wenger, Jan Metzger (ed.): *International CIIP Handbook 2004*, Centre for Security Studies, Zürich 2004.

– ytterst skulle en diskussion om olika generella systemtyper kunna ligga till grund för jämförelsen. Som tidigare konstaterats tycks det dock finnas mycket lite av sådan forskning.

Jämförelsefaktorerna måste därför identifieras induktivt. Utgångspunkten för denna induktiva analys är en nedbrytning av CIP-begreppet, kompletterat med de frågeställningar som de få komparativa studierna betonar[9] samt den empiri som finns i form av diskussioner som förts i olika internationella sammanhang. Denna studies begränsade omfattning innebär dock att det inte är möjligt att diskutera faktorerna i detalj, det handlar snarare om att identifiera tentativa faktorer än att analysera dem. Därmed blir det inte heller möjligt att i detalj studera den forskning som finns kring olika områden som risk- och sårbarhets-analyser eller privat-offentlig samverkan. Detta torde emellertid kunna vara ett område för vidare forskning, inte minst i ljuset av det fördjupade samarbetet inom och utanför EU-ramen på CIP-området.

När det gäller att identifiera EU:s syn på skydd av kritisk infrastruktur är ett problem att det finns ytterst få dokument som explicit fokuserar på CIP. Däremot genomförs redan i dag, inom olika sakpolitikområden, insatser vilka kan ses som CIP. Det krävs därför även en genomgång av CIP-insatser i relevanta sakpolitikområden, som t.ex. informationsteknikområdet, för att analysera EU:s CIP-politik. I föreliggande studie har det inte varit möjligt att göra en fullständig genomgång utan analysen har begränsats till ett urval av politikområden. Utöver detta bör också EU:s övergripande politiska inriktning (fördrag, säkerhetsstrategi, program etc.) tas med i analysen. Detta innebär således en analys av tre olika delar, på delvis tre olika nivåer: Övergripande politisk process, CIP-specifik process samt CIP-relaterat arbete i enskilda politikområden.

För den kontext som är nödvändig för studien – t.ex. rörande utvecklingen av synen på CIP generellt, hotbildsdiskussion, diskussion om aktörs- och icke-aktörsstyrda kriser, konsekvens kontra sannolikhet etc. har studien lutat sig mot tidigare genomfört arbete på FOI. Detsamma gäller till del specifikt svensk syn på skyddet av kritisk infrastruktur.

1.5 Disposition

Rapporten består av fem kapitel utöver detta inledningskapitel. Det nästkommande (kapitel två) identifierar ett antal jämförelsefaktorer vilka sedan i kapitel tre och fyra används för att åstadkomma en strukturerad analys av EU:s

[9] Som tidigare konstaterats är de flesta av dessa utförda av processägare som t.ex. KBM:s s.k. länderstudie (KBM 807/2004) och samma myndighets International CEP Handbook 2003 (SEMA:s Educational Series 2003:2). Ett viktigt undantag är Andreas Wenger, Jan Metzger: CIIP Handbook 2004, Centre for Security Studies, Zurich 2004.

framväxande CIP-politik respektive av svensk CIP-politik. I kapitel fem genomförs därefter en jämförelse mellan EU:s och Sveriges respektive CIP-politik. Kapitel sex utgörs av en avslutande, sammanfattande diskussion.

2 Jämförelsefaktorer

2.1 Allmänt

Fokus för detta kapitel är att finna ett antal jämförelsefaktorer relevanta för att beskriva olika staters och organisationers politik avseende skydd av kritisk infrastruktur. Utgångspunkten är själva begreppet ”skydd av kritisk infrastruktur” ur vilket åtminstone tre övergripande faktorer kan härledas:

- Vad utgör kritisk infrastruktur?
- Mot vad skall denna infrastruktur skyddas?
- Hur skall skyddet utformas?

I de kommande avsnitten skall dessa övergripande faktorer diskuteras vidare och brytas ned i underfaktorer. Studiens omfattning innebär emellertid att det inte finns möjlighet att analysera faktorerna i detalj utan de bör ses som tentativa.

2.2 Vad utgör kritisk infrastruktur?

När Kommissionen genomförde ett seminarium om CIP i juni 2005 visade det sig att urvalet av kritisk infrastruktur var en såväl svår som känslig fråga för medlemsstaterna. Utan en gemensam bild av vad som utgör kritisk infrastruktur i allmänhet, och kritisk infrastruktur på en europeisk nivå i synnerhet, blir det emellertid svårt att utveckla EU-samarbetet på området. Samtidigt visar en genomgång av vad olika stater nationellt rent konkret anser vara kritisk infrastruktur en hög grad av överensstämmelse – det handlar framförallt om tekniska nätverk och grundläggande samhällsverksamheter som t.ex. finanssystem och hälsovård (se bilaga 1). Vad som utgör kritisk infrastruktur är således en grundläggande fråga.

En viktig fråga i EU-diskussionen är vidare vilken infrastruktur som skall anses som kritisk på en europeisk nivå. Ofta påpekas att det bör handla om det som är ”transnationell” eller ”cross-border” infrastruktur, men utan att dessa begrepp tydligt definieras och utan att det tycks finnas någon klar gemensam uppfattning om var gränsen dras mellan nationell och transnationell. Vad som utgör transnationell kritisk infrastruktur är därför en fråga att analysera vidare.

Slutligen varierar graden av systematik och centralisering i identifieringen av kritisk infrastruktur mellan såväl stater som sektorer. Därför blir en fråga hur den kritiska infrastrukturen identifieras och av vem.

2.2.1 Vad utgör kritisk infrastruktur?

Det har föreslagits att vad som utgör kritisk infrastruktur kan förstås utifrån två olika, ej ömsesidigt uteslutande perspektiv: ett symbolperspektiv och ett system-

perspektiv.[10] Det förstnämnda ser en infrastruktur som kritisk beroende på dess, i vid bemärkelse, inneboende egna värde för samhällets ”kritiska nationella intressen” som t.ex. nationell självständighet. I en sådan modell blir eldistribution och kommunikationsnät kritisk infrastruktur men även t.ex. presidenter, regeringsbyggnader och monument.

Det sistnämnda perspektivet ser å sin sida en infrastruktur som kritisk snarare beroende på hur den stödjer andra infrastrukturer i samhället. Då har inte infrastruktur ett egenvärde utan utgör en del av en kedja där enskilda komponenter (elstolpar, transformatorer) bygger upp system (ellinje) som bygger upp en infrastruktur (elnät) som levererar en tjänst (elenergi) som svarar mot ett behov (av energi) för att uppfylla ett mål (tillgång till uppvärmning) som är nödvändigt för att upprätthålla ett grundläggande värde (liv och hälsa, åtminstone på vintern).[11] I en sådan kedja förflyttas fokus för skyddet snarare till de tjänster, varor och flöden som infrastrukturer producerar, och då indirekt de värden dessa står för, än den konkreta infrastrukturen i sig. Systemperspektivet understryker också de beroenden som kan finnas mellan system och hur dessa påverkar tjänster och flöden.

Människor och människors livsbetingelser kommer in på två nivåer i en sådan kedja. För det första är flera av de värden som normalt ses som grundläggande direkt kopplade till människan såsom hälsa, frihet och säkerhet. För det andra kan människor betraktas som en central komponent i system som bygger upp en infrastruktur, och därför kan särskilda grupper behöva skyddas.

2.2.2 Vad utgör transnationell kritisk infrastruktur?

Flera principiellt olika, men inte nödvändigtvis ömsesidigt uteslutande, kriterier kan anläggas för att identifiera vad som är transnationell infrastruktur:

- För det första att det handlar om infrastruktur som är av sådan karaktär att den hjälper till att upprätthålla värden på en över- eller mellanstatlig nivå.
- För det andra att det handlar om sådan infrastruktur vars avbrott kan innebära betydande konsekvenser på en internationell nivå (drabbar mer än en stat), i direkt mening (t.ex. elavbrott i flera länder) eller indirekt (t.ex. genom att orsaka en sådan ekonomisk situation i ett land att ekonomin även drabbas i andra länder).
- För det tredje att det handlar om infrastruktur där det krävs flera stater för att skapa ett rimligt ”försäkringskollektiv” som kan bära en premie, t.ex. i

[10] Jan Metzger: “The Concept of Critical Infrastructure Protection”, i Bailes och Frommelt (red.): *Business and Security*, SIPRI/Oxford University Press, 2004, sid 202f.
[11] Jan Metzger: “Introduction” i Metzger och Wenger (red.): *CIIP Handbook 2004*, Centre for Security Studies, 2004 samt intervju med Jan Lundberg, KBM, juni 2005.

form av reservkapacitet eller i form av förmåga att finansiera återuppbyggnad.

- För det fjärde att det handlar om transnationell infrastruktur i en mer bokstavlig mening, d.v.s. infrastruktur som fysiskt sträcker sig över fler än en stat.

Klart är att mängden transnationell infrastruktur, oavsett hur denna avgränsas, har ökat. Energiöverföring och elektroniska kommunikationer är två exempel på områden där tekniken i allt större utsträckning är gränsöverskridande. Till exempel har avreglering av elmarknaden i Europa lett till en allt större handel med el mellan länder vilket i sin tur skapat ett behov av mer överföringskapacitet mellan länder och således till allt mer integrerade elnät. Samtidigt medför detta att störningar i ett land kan ge följdeffekter i andra länder.[12]

Inom området elektroniska kommunikationer har teknikutvecklingen varit explosionsartad. Det finns idag ett flertal former av mobil telefoni samtidigt som Internet-tekniken har gjort det möjligt att erbjuda ett helt nytt spektrum av nätburna tjänster. Framför allt Internet-tekniken har gjort att betydelsen av traditionella geografiska strukturer försvagats. Rösttrafiken mellan två personer, som sitter i samma land och talar med varandra över telefon, kan idag passera via ett eller flera andra länder.

Parallellt med transnationalisering och avreglering har det också skett en multinationalisering av infrastrukturen och inom flera områden är det vanligt att multinationella företagsgrupper äger system och teknik i flera länder. Några exempel från Sverige är inom energiområdet E.ON, Vattenfall och Fortum, inom elektroniska kommunikationer TeliaSonera, Vodafone och Telenor och inom persontransportområdet Connexgruppen. Genom att centralisera gemensamma och dyrbara funktioner kan en del av dessa företag uppnå stordriftsfördelar. Exempelvis kan drift och övervakning samlokaliseras i ett land. Förmågan att hantera en eventuell kris nationellt påverkas av ett sådant beslut och därmed påverkas även vad som är transnationellt. Om ett multinationellt företag har ett gemensamt, centraliserat ledningssystem placerat i ett land, eventuellt till och med utanför EU, kan detta blir ett argument för att peka ut aktuell infrastruktur som transnationell även om den normalt sett skulle ses som nationell.

[12] Elavbrottet i södra Sverige den 23 september 2003 berodde på störningar i de svenska näten men ledde även till elavbrott i östra Danmark. Italien drabbades av ett större elavbrott den 28 september 2003 beroende på träd som föll på ledningar mellan Schweiz och Italien *Causes of the 2003 Major Grid Blackouts in North America and Europé, and Recommended Means to Improve System Dynamic Performance,* Administrative Committe of the Power System Dynamic Performance Committee, IEEE Power Engineering Society, 2004-08-25, http://psdp.ece.iastate.edu/Blackout_White_Paper_By_IEEE_PES_AdComm_FINAL_082504.pdf.

2.2.3 Hur identifieras kritisk infrastruktur och av vem?

Graden av systematisk analys i processen att identifiera kritisk infrastruktur är en viktig faktor.[13] Identifiering av kritisk infrastruktur sker ofta utifrån ett konsekvensperspektiv med faktorer såsom konsekvens av bortfall för grundläggande samhällsvärden och/eller samhällsintressen, beroenden samt möjligheten att tillgodose samhällets behov via andra vägar.[14] I det faktiska urvalet av vad som anses vara kritisk infrastruktur väger emellertid även staters tradition och förutsättningar in. Detta är mindre förvånande eftersom hur ett samhälle och dess befolkning upplever konsekvenser och tidsutdräkt kan variera. Till exempel lägger ett land som Nederländerna stor tyngd vid reglering av vattennivåer vilket med tanke på geografin är naturligt.

Huruvida identifiering av kritisk infrastruktur sker uppifrån och ned eller nedifrån och upp är en annan faktor. En process som är uppifrån och ned utan systematisk analys ger en styrd, deduktivt nedbruten identifiering – på varje nivå görs ett urval och prioriteringar av infrastruktur på grundval av de prioriteringar som beslutats på nivån närmast ovanför. En process som är nedifrån och upp med analys ger istället en icke-styrd, induktivt uppbyggd identifiering – varje nivå måste syntetisera och väga av ett antal analysgrundade resultat från nivån närmast under. Resultaten av dessa kan bli mycket olika till sin karaktär och därmed också svåra att relatera till varandra. Detta accentueras i en situation där prioriteringar sedan skall ske på en europeisk nivå.

På vilket sätt privata aktörer deltar i processen att identifiera kritisk infrastruktur är en fråga aktuell visavi såväl nationell som transnationell (i denna rapport europeisk) infrastruktur. Det berör i en vid mening samverkan mellan samhälle och näringsliv, och ytterst vem som skall ansvara för finansiering av skyddsinsatser. När det gäller europeisk infrastruktur tillkommer dessutom frågan om det är EU eller medlemsstaterna som skall ansvara för kontakter med näringslivet.

---

[13] CIIP Handbook 2004 går igenom ett antal olika metoder för analys av framförallt kritisk informationsinfrastruktur. Bland annat presenteras ”impact analysis”, på svenska effekt analys, d.v.s. analys av vilken effekt ett avbrott eller skada på en viss infrastruktur skulle få för samhället. Metzger och Wenger (red.): *CIIP Handbook 2004*, Centre for Security Studies, 2004.

[14] Se Commission of the European Union: *Critical Infrastructure Protection in the Fight against terrorism*, COM(2004) 702, 2004-10-20 samt Birgitta Lewerentz et al: *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system*, FOI MEMO 1283, mars 2005.
FOI-studien utgick från ett antal grundläggande värden som de identifierat ur bl.a. EU-dokument, försvarspropositioner och försvarsberedningsrapporter: frihet, demokrati, rättsstatsprincipen, respekt för mänskliga rättigheter, respekt för människans värdighet. Dessa uppbärs i sin tur av ett antal för samhället vitala intressen: värnandet av liv och hälsa, värnandet av miljön, upprätthållandet av en god samhällsekonomi och skydda ekonomiska värden, upprätthållandet av en demokratisk rättsstat samt bevarandet av fred och självständighet. För dessa respektive vitala samhällsintressen identifierades sedan ett antal konkreta infrastruktursystem som penningsystem, transportsystem, informationssystem etc. vilka levererade nödvändiga tjänster. Utifrån en analysstruktur av det slag som presenteras i brödtexten gjordes slutligen en samlad bedömning av aktuell verksamhets vikt för de grundläggande värdena.

2.3 Mot vad skall kritisk infrastruktur skyddas?

Vilken hotbild man utgår från är, eller bör vara, grundläggande för hur skyddet utformas. Vad som betraktas som relevanta hot är därför en i stort självklar faktor för detta slags jämförande analys. Eftersom hotbildsbedömningarna i hög grad blir styrande för skyddsinsatserna blir närbesläktade, och särskilt i ett internationellt sammanhang viktiga faktorer hur dessa bedömningar genomförs och av vem.

2.3.1 Vad betraktas som relevanta hot?

Hotet kan bedömas utifrån olika grunder – konsekvensen av att något inträffar kan vara lika viktigt som sannolikheten för att det inträffar. För Europa har de icke-aktörsstyrda kriserna haft högst sannolikhet: översvämningar, stormar, jordskred etc. Trots detta är det aktörsstyrda händelser som tenderar att komma i fokus för den europeiska diskussionen om skydd av kritisk infrastruktur, särskilt då terrorism. Ett skäl kan vara att konsekvenserna – såväl de konkreta i form av förstörelse och effekter för samhällets funktion som de mer svårmätbara som t.ex. psykologiska – i sig kan bli oacceptabelt stora i terrorismfallet. Det är vidare möjligt att den säkerhetspolitiska dimensionen hos terrorism påverkar hur behovet av ett övergripande samhällsansvar uppfattas.

Det är i detta sammanhang också en relevant fråga huruvida infrastruktur verkligen utgör ett intressant mål för terrorism. Dåden mot Madrids och Londons tunnelbanor, liksom sprängdådet mot Londons finanskvarter april 1992 och ett antal av de senaste årens virusattacker på nätet[15], visar att system som anses som kritisk infrastruktur kan bli måltavlor. Frågan är dock om det är deras roll som kritisk infrastruktur som är den primära anledningen till målvalet. Att attackera tunnelbanan kan lika gärna handla om att det är ett taktiskt relativt enkelt sätt att maximera antalet offer samtidigt som det genererar stora psykologiska effekter som att det är ett strategiskt sätt att få transportsystemet att bryta samman. Samtidigt kan frågan huruvida ett mål är valt utifrån hur kritiskt det är eller utifrån andra aspekter tendera att blir mer akademisk. För de flesta ”kritiska” infrastrukturer innebär det stora konsekvenser om de slås ut, det ligger i deras natur. Skillnaden kan sägas vara att dåd för att till fullo dra nytta av att en infrastruktur är kritisk och därigenom att åstadkomma strategiska effekter kräver ett antal större och bättre samordnade insatser än om man bara vill åstadkomma kortsiktiga, taktiska effekter.[16]

[15] Malin Fylkner et al.: *Aktörer, antagonister och angrepp – En studie om det kvalificerade IT-hotet*, FOI-R--1182--SE, februari 2004.

[16] VITA-projektet (Vital Infrastructure Threats and Assurance) inom ramen för EU:s förberedande säkerhetsforskningsprogram arbetar bl.a. att försöka definiera möjliga och trovärdiga hot mot kritisk infrastruktur som är av en sådan karaktär att de blir en fråga för mer än bara den drabbade staten.

Ytterligare en aspekt av vad man betraktar som hot är hur man skiljer den dagliga, ”normala” hotbild som all infrastruktur lever under (brottslighet, dataintrång, olyckor etc.) från det som utgör ett hot som är en angelägenhet för det allmänna. Fördelningen av ansvar och ekonomiska skyldigheter kan se väldigt olika ut beroende på hur gränsen mellan ”normalt” och ”extraordinärt” dras. Det gäller särskilt när hotet också får en säkerhetspolitisk dimension.

Olika sektorer kan vidare värdera hoten olika. Medan hotet från terrorism är högst reellt för flygtransportsektorn är det möjligen mindre överhängande för livsmedelssektorn.[17] Även olika medlemsstater lever under delvis olika hotbilder. Det gäller såväl aktörsstyrda som icke-aktörsstyrda hot. För Nederländerna är hotet från havet i form av översvämningar högst reellt, i Spanien är istället hotet från större skogsbränder i fokus. I Sverige uppfattas hotet från terrorism som betydligt lägre än vad som är fallet i ett Storbritannien aktivt i Irak. För Sverige utgör kyla och snö ett centralt hot mot svenska elnät medan det är betydligt mindre relevant för det spanska eldistributionssystemet. Detta slags skillnader kan komplicera sammanvägningen av bedömningar av hotet på EU-nivå, och naturligtvis även i nästa steg vilka skyddsåtgärder som bör prioriteras.

2.3.2 Hur definieras hotet och av vem?

På nationell nivå handlar denna fråga bland annat om huruvida det finns en centralt formulerad, normerande hotbild eller om varje infrastruktursektor ansvarar för utvecklandet av sin egen hotbild. Frågeställningen kopplar också till diskussionen om hur olika sektorer och stater kan uppfatta hotbilden olika (avsnitt 2.3.1).

Frågeställningens betydelse accentueras på den internationella nivån. Upptakten till Irakkriget visade hur olika medlemsstater kan uppfatta hotet i en specifik situation. Gemensamma strukturer för sammanställning av och diskussioner kring underrättelser och hotbild skulle emellertid kunna bidra till en mer enhetlig uppfattning av en situation, byggd på en gemensamt ägd analys. Detta utesluter inte skilda politiska tolkningar men ger åtminstone möjligheter för en ökad grad av samsyn.[18]

Eftersom tolkningen av information och underrättelser snabbt blir politik finns det bland stater emellertid traditionellt en olust inför allt för mycket av centrala bedömningar – stora stater vill inte lämna ifrån sig den makt som kunskap och tolkningsföreträde innebär medan små stater kan känna rädsla för att bli styrda. Samtidigt kan bara det faktum att man i gemensamma forum diskuterar och

[17] Det finns dock fall av ”matterrorism”, ett uppmärksammat exempel var då palestinska terrorister för drygt 20 års sedan påstod sig ha sprutat kvicksilver i israeliska jaffa-apelsiner.

[18] I en EU-kontext skulle de EU-strukturer som har uppgifter rörande underrättelser, såsom t.ex. Rådssekretariatets lägescentral (Situation Centre), polissamarbetet EUROPOL eller de olika varningsnätverken, ha en sådan roll.

utvärderar information göra det lättare för små stater att värdera de informationsbitar de stora lämnar ifrån sig. I det vanliga underrättelsesamarbetet – ofta bilateralt eller ”fålateralt” – kan detta vara svårare.

2.4 Hur skall skyddet utformas?

Detta är den mest komplicerade faktorn att bryta ned då den innehåller en mängd olika aspekter. Eftersom det är de sektorsövergripande jämförelsefaktorerna som är i fokus för denna studie ligger tyngdpunkten dock på faktorer som berör den principiella utformningen av skyddet, särskilt ur ett internationellt perspektiv.

En sådan potentiellt särskiljande faktor utgörs av vilket slags insatser för skydd av kritisk infrastruktur ett land eller organisation prioriterar. Detta kan också formuleras som i vilken fas av skyddsarbetet man lägger tyngdpunkt på.

I ett internationellt sammanhang blir det också centralt vilken karaktär och roll man kan tänka sig att se för i någon mening multinationellt överenskomna skyddsinsatser. Här tycks det finnas betydande skillnader mellan olika stater och organisationer.

Vidare är frågan om vem som ansvarar för skyddet av kritisk infrastruktur grundläggande – detta berör både ansvarsfördelningen mellan olika nivåer (multinationell, nationell, lokal) och ansvarsfördelningen mellan privat och offentligt. Närbesläktat med detta är synen på hur CIP-åtgärder skall finansieras.

2.4.1 Vilken fas av skyddsarbetet lägger man tonvikten på?

Skydd av kritisk infrastruktur kan ske i olika faser: Förebyggande (att se till att undanröja orsaken till en potentiellt skadlig händelse eller minska effekten av en sådan händelse), beredskap och förberedelser (planera och träna för att hantera konsekvenserna av händelser som inte kan förebyggas), faktisk hantering av situation där händelse inträffat (den direkta hanteringen av händelses konsekvenser, t.ex. att få igång ersättningsstruktur) samt återhämtning (där infrastrukturen återställes).[19] Även om olika typer av hot, och olika typer av skyddsobjekt, kräver olika tyngdpunkt hos skyddet kan det också finnas skillnader mellan olika aktörer avseende vilken fas man prioriterar.

Närbesläktat är vilken koppling skyddet av kritisk infrastruktur har till ett övergripande krisberedskapstänkande. Är CIP en del av en övergripande strategi för samhällets säkerhet eller är det ett politikområde som ”står för sig själv”? Även om man inte behöver gå så långt som vissa bedömare gör, och hävda att det

[19] Anpassat från Willi Stein: *Role of IT in Critical Infrastructure Protection (CIP) and Emergency Situations*, September 2003, hämtad 2005-05-25 från www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec/wilbert.html.

flesta stater inte har någon övergripande strategi för skydd av kritisk infrastruktur,[20] är det uppenbart att det finns en stor variation i omfång mellan olika staters strategier. Brister eller skillnader i strategi kan leda till svårigheter i att åstadkomma en gemensam, strukturerad analys av hot, skyddsbehov och skyddsobjekt. Därmed blir det också svårt att hantera de skillnader i tradition som finns mellan olika staters arbete med CIP.

2.4.2 Vilken karaktär skall multinationella åtgärder för skydd av kritisk infrastruktur få?

Synen på vilken karaktär eventuella gemensamma, multinationella åtgärder för skydd av kritisk infrastruktur skall få kan variera. Den kan sträcka sig från icke-bindande rekommendationer till gemensamma regelverk, från utbyte av erfarenheter till skapandet av gemensamma, överstatliga regimer för skyddsarbetet, från frivilligt samarbete till centralt övervakade regelverk och sanktioner.

Synen på multinationella åtgärders karaktär kan också variera mellan olika sektorer. Till exempel är flygsäkerhet ett område där det är viktigt att alla stater håller samma säkerhetsnivå och där det därför tycks lättare att ha styrande regelverk och internationella inspektioner. Verksamheten finns också inom relativt väldefinierade, enhetliga ramar och det finns ett starkt affärsmässigt intresse av att upprätthålla säkerheten. När det gäller t.ex. skydd av informations- och kommunikationsnät är öppenheten för styrande regelverk möjligen mindre, verksamheten mer heterogen och det affärsmässiga intresset av att upprätthålla skyddsnivåer mindre.

Acceptansen för gemensamma regelverk kan möjligen också variera för olika faser i CIP-arbetet. För många stater är det troligen lättare att acceptera gemensamma miniminivåer för förebyggande åtgärder än t.ex. gemensamma normer för det operativa hanterandet av t.ex. återställande eller ersättande av infrastruktur.

Ytterst handlar denna fråga om vilket inflytande stater är beredda att ge till en över- eller mellanstatlig nivå när det gäller skyddet av kritisk infrastruktur. Ju mer av styrande beslut, desto mer av internationellt inflytande över nationell hantering av kritisk infrastruktur. Detta gäller även i en EU-kontext.

2.4.3 Vem ansvarar för skyddet av kritisk infrastruktur?

De flesta stater, inklusive Sverige, menar att skyddet av kritisk infrastruktur är en i första hand nationell fråga. Transnationaliseringen och multinationaliseringen av infrastruktur har dock inneburit att det blir allt svårare att skilja på vad som är rent nationell infrastruktur och vad som är strukturer av en sådan

[20] Stefan Ritter, Joachim Weber: Critical Infrastructure Protection: *Survey of world-wide Activities*, September 2003, hämtad 2005-05-17 från www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/pubonl/reinermann.

karaktär att det krävs ett fördjupat internationellt samarbete, från gemensamma normer och regler till överstatlig tillsyn och ansvar för dess skydd. Här finns också en dynamik – ju mer globaliserad en tjänst eller infrastruktur blir desto större behov av samarbete kring säkerhetsfrågorna.

Parallellt med denna utveckling har i Sverige, liksom i växlande utsträckning i resten av Europa, under det senaste decenniet genomförts omfattande avregleringar av större infrastruktursystem. Tjänster som telefoni, eldistribution och järnvägstransporter erbjuds nu på en avreglerad marknad med privata aktörer. Även om viss grundläggande infrastruktur fortsatt ligger hos statliga eller statligt ägda aktörer (t.ex. kopparaccessnätet hos Teliasonera, järnvägsrälsen hos Banverket)[21] är tjänsteleverantörer privata. Inom vissa områden, som t.ex. mobiltelefoni, är såväl tjänsteleverantörer som infrastrukturägare huvudsakligen privata.

Detta innebär att nationalstatens roll blivit mer oklar. Å ena sidan har skyddet av kritisk infrastruktur blivit allt mer en fråga som kräver gemensamma, multinationella synsätt och beslut. Å andra sidan får privata företag i allt högre grad ansvaret för skyddet av samhällets kritiska infrastruktur och de verksamheter dessa upprätthåller. Sammantaget handlar detta om en balansgång mellan nationellt självstyre, fri företagsamhet och behovet av bra och likformiga skyddsnivåer över nationsgränserna. En viktig faktor är därför hur ansvarsfördelningen ser ut mellan den internationella nivån, den nationella nivån och ägare/operatörer för olika typer av åtgärder för nationell respektive transnationell infrastruktur. I en diskussion kring detta behöver man även skilja på ansvaret för skydd av kritisk infrastruktur inom en enskild sektor och det sektorsövergripande ansvaret.

Liksom var fallet med hot- och riskanalyser och identifiering av kritisk infrastruktur blir en central fråga vilken nivå som skall ansvara för samarbetet med ägare/operatörer. Särskilt komplicerat kan detta bli om infrastrukturen är privat ägd i vissa stater medan den är offentligt ägd i andra. Tidigare fanns det i de flesta länder ett statligt monopol som ansvarade för telefonin och ansvarsområdena var därför avgränsade och tydliga. Idag är i flertalet stater dessa monopol borta, marknaden är avreglerad och konkurrensutsatt. Handlar det dessutom om multinationella företag kan, som tidigare noterats, ledning och kontroll över verksamheten sitta i en stat medan själva infrastrukturen finns i andra.

Närbesläktat med detta är hur samverkan mellan det offentliga och näringslivet skall se ut. I en KBM-rapport[22] pekar Jan Joel Andersson och Andreas Malm ut fyra huvudskäl till varför näringsliv inte på egen hand tar tillräckligt ansvar för

[21] Även detta förändras emellertid – ett exempel är hur utbyggnaden av bredband skapat ett nytt alternativt accessnät för teletrafik.
[22] Jan Joel Andersson, Andreas Malm: *Mind the gap!*, KBM:s temaserie 2005:8, sidan 10ff.

krisberedskap, inklusive skydd av infrastrukturen: För det första blir skyddet en kollektiv nytta, på samma sätt som försvar och rättsväsende, som är svår att ta betalt för varför företag inte kommer att producera denna. För det andra att det inte är företagen som producerar en tjänst som bär huvuddelen av kostnaden när denna tjänst råkar ut för ett avbrott, d.v.s. kostnaden för att skydda tjänsten ställs inte mot hela samhällskostnaden för ett avbrott. För det tredje att företag inte har resurser för en övergripande analys av hot, risker och vad som utgör acceptabel krisberedskap. För det fjärde att företag ”förväntar sig” att staten räddar dem vid en kris och därför inte är motiverade till satsningar på den typ av ”försäkring” som en investering i krisberedskap innebär.

För att påverka ägare/operatörer krisberedskapsarbete kan staten införa lagreglerade säkerhets- och skyddsnivåer, ekonomiska morötter eller ingå privat-offentliga partnerskap. Andersson och Malm menar dock att sådant partnerskap utan tydliga riktlinjer och utan ekonomisk kompensation från staten till ägare/-operatörer är en problematisk och osäker väg för att öka skyddsnivån. De riskerar att fungera som en avledande åtgärd där man visserligen är överens om problemet men inte definierar vem som har ansvaret att göra något åt det.[23]

En ytterligare aspekt är det sektorsövergripande CIP-systemets grad av centralisering alternativt decentralisering. I ett centraliserat system sker den sektorsövergripande koordinationen, samverkan och prioriteringen av resurser mellan olika sektorer från en punkt som, i bästa fall, sitter på en övergripande bild av hot, sårbarheter och resurser. Ett decentraliserat system bygger istället på principen att behovet av skydd bäst avgörs av lokala nivån. I realiteten är de flesta system blandformer. I ett decentraliserat system krävs förmåga att samla resurser och hantera kriser rationellt när de berör mer än en lokal punkt. I ett centraliserat system krävs lokal organisation som analyserar och utför skyddsåtgärderna.

2.4.4 Hur finansieras skydd av kritisk infrastruktur?

Finansiering av åtgärder relaterat till CIP kan ske på en rad olika vis. För det första genom att ägare/operatör frivilligt eller lagstyrt finansierar skyddet av sin infrastruktur. För det andra genom att ansvarig statlig eller internationell nivå tar in avgifter som används för att finansiera skyddsinsatser. För det tredje genom att ansvarig statlig eller internationell nivå anslagsfinansierar åtgärder för skydd av kritisk infrastruktur.

Olika finansieringsvägar kan vara olika attraktiva för olika typer av åtgärder. Tvingande, egenfinansierade åtgärder kan vara lättare att se för fysiskt skydd av infrastruktur, särskilt om detta skydd även behövs för att hantera normala stör-

[23] Ibid, sidan 15ff.

ningar och brottslighet, än t.ex. system särskilt inriktade för att identifiera bioterrorism i tunnelbanesystem, som kan ses som ett samhällsansvar.

Synen på finansieringsformerna kan också variera såväl mellan olika sektorer som mellan olika stater, t.ex. beroende på tradition, grad av privatisering etc. En viktig faktor i graden av acceptans hos ägare/aktörer för att ta kostnaderna för skyddsåtgärder kan t.ex. vara i vilken grad det är i en mer konkret mening affärsmässigt motiverat – flygbranschens känslighet för olyckor och terrordåd gör den villigare att investera i skyddet.

2.5 Sammanfattning av jämförelsefaktorer

Den samlade listan över jämförelsefaktorer blir som följer:

- Vad utgör kritisk infrastruktur?
    - Vad utgör kritisk infrastruktur?
    - Vad utgör transnationell kritisk infrastruktur?
    - Hur identifieras kritisk infrastruktur och av vem?
- Mot vad skall kritisk infrastruktur skyddas?
    - Vad betraktas som relevanta hot?
    - Hur definieras hotet och av vem?
- Hur skall skyddet utformas?
    - Vilken/vilka faser i skyddsarbetet lägger man tonvikten på?
    - Vilken karaktär skall multinationella åtgärder för skydd av kritisk infrastruktur få?
    - Vem ansvarar för skyddet av kritisk infrastruktur?
    - Hur finansieras skydd av kritisk infrastruktur?

3 EU och skydd av kritisk infrastruktur

3.1 Allmänt om EU:s processer rörande skydd av kritisk infrastruktur

För att studera hur EU förhåller sig till skydd av kritisk infrastruktur krävs en analys på tre olika politiknivåer: De övergripande politiska processerna, de specifika processerna för utveckling av en europeisk CIP-politik samt de CIP-relaterade processerna i enskilda sakpolitikområden.

I detta kapitel presenteras först översiktligt beslut och åtgärder i de olika processerna. Därefter görs en analys av EU:s framväxande CIP-politik utifrån de tidigare identifierade jämförelsefaktorerna.

Gränslinjen mellan vad som faller inom de olika nivåerna är bitvis svårdefinierad. För att inte hamna i onödiga, och för läsaren tröttsamma, gränsdragningsdiskussioner har här en indelning gjorts på ett pragmatiskt, intuitivt sätt – där en process passar bäst i övrig kontext har den också placerats.

3.1.1 Övergripande politiska processer

Sedan 2001 är det fyra övergripande, politiska processer som står ut på säkerhetsområdet och som kopplar till skydd av kritisk infrastruktur. Den första är arbetet med det nya konstitutionella fördraget[24], den andra är utvecklingen av en europeisk säkerhetsstrategi[25], den tredje är framtagandet av Haagprogrammet för inre säkerhet[26] och den fjärde är arbetet med handlingsplanen för terrorismbekämpning[27]. Till dessa fyra kan också läggas införandet av den så kallade solidaritetsfonden.

Fördragsutkastet lägger ett ramverk i vilket utrymmet för samarbete på EU-nivån avseende skydd och säkerhet utökas. I fördragsutkastet fastställs också Unionens övergripande mål som att bl.a. ”främja freden, sina värden samt folkens välfärd” men även att erbjuda sina medborgare ”ett område med frihet, säkerhet och rättvisa” och ”en inre marknad, där det råder fri och icke

[24] ”Fördraget om upprättandet av en konstitution för Europa”, *Europeiska Unionens Officiella Tidning C310*, 2004-12-16. Processen att ratificera fördraget har avstannat efter det att medborgarna i flera medlemsstater markerat att de inte är nöjda med förslaget. Emellertid var EU:s stats- och regeringschefer överens om den kompromiss som fördragsutkastet innebär och när ett nytt fördrag till slut blir verklighet kommer det med stor sannolikhet att ligga nära dagens utkast.
[25] Javier Solana: *A Secure Europe in a Better World*, EU/Bryssel 2003-12-12.
[26] The Council: “The Hague Programme: Strengthening freedom, security and justice in the European Union.” *Europeiska Unionens Officiella Tidning* C53, 2005-03-03.
[27] Se Council of the European Union: *Coordination of implementation of the plan of action to combat terrorism*, 12800/01, 2001-10-17. Själva handlingsplanen mot terrorism antogs 21 september 2001.

snedvriden konkurrens". I definitionen av grundläggande värden som EU omfattar ingår bl.a. frihet, demokrati och rättsstatsprincipen.[28]

Fördragsutkastets innehåller vidare en så kallad solidaritetsklausul rörande naturkatastrofer och terrordåd i vilken EU:s medlemsstater lovar varandra hjälp, med alla medel inklusive militära, för att förhindra terrorhot på Unionens territorium, för att skydda civilbefolkning och demokratiska institutioner från terroristattacker samt för att på begäran bistå en medlemsstat på dess territorium vid ett terrordåd eller en naturkatastrof.[29]

I fördragsutkastet införs också en så kallad operativ kommitté med uppgift att främja det operativa samarbetet inom Unionen rörande inre säkerhet. Denna kommitté skall "främja samordningen av de åtgärder som vidtas av medlemsstaternas behöriga myndigheter".[30] Operativa kommittén får vidare en roll i förhållande till solidaritetsklausulen, där kommittén tillsammans med Kommittén för utrikes- och säkerhetspolitik (KUSP) skall biträda Rådet i att ta fram föreskrifter för hur solidaritetsklausulen skall tillämpas.

Säkerhetsstrategin utgör ett slags "verksamhetsidé" för EU:s framförallt externa säkerhetsarbete och definierar en gemensam syn på hur, när och för vilka syften EU skall agera. Ett genomgående tema i strategin är hur för EU intern och extern säkerhet blivit allt närmare sammanbundna. Även i säkerhetsstrategin talas det om europeiska värden.

I november 2004 antog Rådet vidare det så kallade Haag-programmet, en övergripande politisk strategi för att "stärka frihet, säkerhet och rättvisa i Europeiska Unionen".[31] Programmet utgör en hatt under vilken samlats ett antal olika åtgärder, vilka syftar till att stärka hela området för inre säkerhet. När det gäller skydd av kritisk infrastruktur understryks att EU måste bli bättre på att hantera kriser som har transnationella effekter, inklusive sådana som berör "vital infrastruktur". I programmet ingår bl.a. inrättandet av "integrerade och koordinerade krishanteringsarrangemang i Unionens institutioner". Häri innefattas bl.a.

---

[28] "Fördraget om upprättandet av en konstitution för Europa", *Europeiska Unionens Officiella Tidning* 2004-12-16, C310, paragraferna I-3 och I-4.

[29] I uttalandet efter terrordåden i Madrid enades EU:s Medlemsstater kring de delar av solidaritetsklausulen som berör terrorism även om fördragsutkastet i övrigt inte ratificerats. "Fördraget om upprättandet av en konstitution för Europa", *Europeiska Unionens Officiella Tidning C310*, 2004-12-16, artikel I-43 och III-329.

[30] "Fördraget om upprättandet av en konstitution för Europa",, *Europeiska Unionens Officiella Tidning C310*, 2004-12-16, artikel III-261. Denna kommitté utgör en utveckling av det nuvarande fördragets "samordningskommitté" (den så kallade artikel 36 kommittén) som syftade till att "bistå" Rådet i samordningsfrågor men med en troligen mer operativ roll.

[31] The Council: "The Hague Programme: Strengthening freedom, security and justice in the European Union." *Europeiska Unionens Officiella Tidning* C53, 2005-03-03. Beslutet fattades 2004-11-05. Se också Eva Hagström Frisell, Maria Oredsson: *EU response to crisis – the role of military resources* (kommande FOI-rapport).

arrangemang för att fortsatt värdera medlemsstaternas kapaciteter, utbildning, övningar, förlagring av materiel, och operativa planer för civil krishantering.[32]

Kommissionen lade i april 2005 fram ett förslag till ramprogram ”för säkerhet och skydd av friheter” bl.a. som ett svar på en begäran i Haagprogrammet om ett program för förebyggande och konsekvenshantering av terrorism.[33] Programmet skall ”bidra till att skydda medborgare, deras friheter och samhället mot terroristattacker och relaterade händelser, och skydda EU som ett område av frihet, säkerhet och rättvisa, genom att stimulera, stödja och utveckla åtgärder rörande förberedande och konsekvenshantering”.[34] Kommissionen vill bl.a. se stöd till samarbets- och koordinationsmekanismer. När det gäller förebyggande av och förberedelser inför terrordåd skall programmet stödja utvecklingen av risk- och hotanalyser rörande kritisk infrastruktur, av gemensamma säkerhetsstandarder och erfarenhetsutbyte samt koordinationen rörande skyddet av kritisk infrastruktur.[35]

EU antog 2001 en handlingsplan för terroristbekämpning som innehöll ett brett spektrum av olika slags åtgärder: utbyggt rättsligt samarbete, insatser för att stoppa finansiering av terrorism, ökat samarbete inom räddningstjänstområdet etc.[36] I Europeiska Rådets uttalande efter Madriddådet 2004 ingick en reviderad handlingsplan för terrorismbekämpning.[37] Denna identifierade sju huvudmålsättningar varav två var kopplade till CIP: att öka säkerheten för internationella transporter och skapa säkra gränsskyddssystem samt att förbättra EU:s och medlemsstaternas kapacitet att hantera konsekvenserna av ett terrordåd. I det sistnämnda ingick även framtagandet av en strategi för skyddet av kritisk infrastruktur och stärkt skydd för medborgare och grundläggande samhällstjänster.[38]

I den övergripande politiknivån bör även den så kallade solidaritetsfonden räknas in. Denna inrättades av EU 2002 med syftet att kunna ge stöd till medlemsstater som drabbats av en omfattande naturkatastrof. Fonden skall bl.a. kunna bidra till att hjälpa en drabbad stat att åstadkomma omedelbart återställande av infrastruktur (inklusive energi, vatten, transporter etc.) och att sätta

[32] Ibid, avsnitt 2.4.
[33] Commission of the European Communities: *Communication from the Commission to the Council and the European Parliament Establishing a framework programme on “Security and Safeguarding Liberties” for the period 2007-2013*, COM(2005)124 Final, 2005-04-06. Ramprogrammet är tänkt att innehålla ca 7,5 miljarder kronor under den aktuella perioden och hjälpa till att finansiera projekt inom ramen för programmets syften.
[34] Ibid, sid 14.
[35] Ibid, sid 14.
[36] Se Council of the European Union: *Coordination of implementation of the plan of action to combat terrorism*, 12800/01, 2001-10-17. Själva handlingsplanen mot terrorism antogs 21 september 2001.
[37] Council of the European Union: *Declaration on Combating Terrorism*, 2004-03-25.
[38] Ibid. De andra huvudmålsättningarna var att utveckla de internationella ansträngningarna för kampen mot terrorismen, minska terroristernas tillgång till finansiering, maximera Unionens kapacitet att upptäcka, utreda och döma terrorister, bekämpa de faktorer som leder till stöd för och rekrytering till terrorism samt stöd till tredje land i kampen mot terrorism.

upp tillfälliga skydd och annat stöd till drabbade.[39] Detta utgör således ett slags försäkringsfunktion på Unionsnivån där EU delar på kostnaden vid vissa exceptionella situationer.[40]

Den övergripande politiska processen i EU har hittills bara i begränsad omfattning explicit berört CIP. Dokument och initiativ innehåller dessutom lite av hårda beslut utan fokuserar på att understryka att problemen är gemensamma, att EU:s medlemsstater behöver finna mekanismer för att hantera dessa problem på ett rationellt sätt och att stimulera utvecklingen av en gemensam grundsyn. Haagprogrammet betonar också ett flertal gånger att medlemsstaterna måste agera inte bara för sin egen nationella säkerhet utan fokusera på Unionens sammanlagda säkerhet. EU:s roll anges vara att stå för överblick och samordning av kompetenser och andra resurser och att kunna samordna dess utnyttjande i en kris. EU skall fungera som katalysator för ett ytterligare närmande mellan medlemsstaterna och skall ”stimulera” eller ”stödja” ökat samarbete, inte styra.

I linje med detta inrättas inte något centralt ”krishanteringsorgan” inom EU. Däremot sker nu en utveckling av de ”integrerade krishanteringsarrangemang” som efterlyses i Haagprogrammet. Arrangemangen kommer troligen att ha en roll att i en kris dels skapa samsyn mellan Kommission, Rådssekretariat och medlemsstater, dels koordinera insatser och information. Dessutom skapas i Kommissionen ett för Kommissionen centralt kriscenter med deltagande från alla för krisen relevanta delar av Kommissionen. Kommissionen avser också att upprätta ett system för snabb varning, ARGUS, som skall sammanfoga alla de system som idag finns inom Kommissionens olika sakpolitikområden.[41]

3.1.2 Processer specifikt inriktade på skydd av kritisk infrastruktur

Utveckling av den CIP-specifika politiken sker i två, nära sammantvinnade spår – i det första ingår CIP som en del av EU:s arbete att förbättra förmågan att möta och hantera terrorism, i det andra driver Kommissionen en process att ta fram ett förslag till europeiskt program för CIP, EPCIP (European Programme for Critical Infrastructure Protection).

Efter den 11 september 2001 har terrorismbekämpning kommit att fungera som en katalysator för utvecklingen av EU:s samlade arbete med krishanterings-

[39] “Council Regulation (EC) No 2012/2002 of 11 November 2002 establishing the European Union Solidarity Fund”, *Europeiska Unionens Officiella Tidning, L 311/3*, 2004-11-14.
[40] Sverige fick t.ex. ca 780 miljoner i stöd för att hantera konsekvenserna av stormen Gudrun januari 2005.
[41] Commission of the European Union: *Preparedness and consequence management in the fight against terrorism*, COM(2004) 701, Brussels 2004-10-20, sidan 11. Se också Eva Hagström Frisell, Maria Oredsson: *EU response to crisis – the role of military resources* (kommande FOI-rapport).

frågor, inklusive CIP.[42] Utöver de kopplingar som kan göras till CIP i handlingsplanen för terrorismbekämpning antog EU 2002 det så kallade CBRN-programmet för ökat samarbete mellan medlemsstaterna, Rådet och Kommissionen rörande olika aspekter av hanteringen av CBRN-hotet.[43] Den reviderade handlingsplanen för terrorismbekämpning efter Madriddåden[44] innehöll en anmodan om uppdatering och vidgning av CBRN-programmet till alla typer av terrorism. Det kom att benämnas ”Solidaritetsprogrammet” och kopplades till handlingsplanens huvudmålsättning ”att förbättra EU:s och medlemsstaternas kapacitet att hantera konsekvenserna av ett terrordåd”, men kom att beröra mer än bara konsekvenshantering.[45]

Solidaritetsprogrammet innehåller sex så kallade ”strategiska mål”:

- förstärkt förmåga till analys och värdering av risker och sårbarheter för potentiella mål,
- förebyggande och sårbarhetsreducerande åtgärder inklusive skydd av kritisk infrastruktur,
- detektering och identifiering av hot,
- förberedelser och konsekvenshantering,
- forskning och utveckling,
- internationellt samarbete med tredje land.

Dessa mål skall uppnås genom fördjupad koordination och samarbete mellan medlemsstater, Rådet och Kommissionen, genom underlättande av stöd till medlemsstater om de så begär samt genom ett samordnat utnyttjande av EU-instrument, inklusive tillskapandet av nya instrument om det visar sig nödvändigt. Programmet understryker att medlemsstaterna har det främsta ansvaret för skyddet mot terrorism och EU-organens roller beskrivs framförallt som ”att uppmuntra” åtgärder, ”rekommendera” riktlinjer eller ”att bidra till utbyte av erfarenheter”.

CBRN-programmet och solidaritetsprogrammen, liksom den tidigare nämnda handlingsplanen för terrorismbekämpning, är politiska program som beskriver en politisk inriktning och som under en hatt samlar ett antal åtgärder som beslutats, eller skall beslutas, i andra sammanhang. Deras fokus är i samtliga tre

[42] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, sidan 17f.
[43] Council of the European Union: *Adoption of the programme to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats*, 14627/02, 2002-11-21.
[44] Council of the European Union: *Declaration on Combating Terrorism*, 2004-03-25.
[45] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01.

fall terrorism, d.v.s. inte all-hazards. Samtidigt görs kopplingar i Solidaritetsprogrammet till t.ex. EPCIP som är – eller har potential att vara – mer generellt avseende hot.

Vid EU:s toppmöte maj 2004 beslöt EU:s stats- och regeringschefer att be Rådet, på grundval av en mellan SG/HR och Kommissionen koordinerad approach, ta fram en europeisk strategi för skyddet av kritisk infrastruktur.[46] Detta utgjorde den formella starten av den specifika processen att ta fram ett program för CIP i EU. Arbetet kan ses som ett utskott från arbetet med kampen mot terrorismen men har med tiden fått en mer allmän karaktär inriktad mot ”all-hazards”.

Kommissionen presenterade i oktober 2004 tre meddelanden vilka i olika omfattning berörde skydd av kritisk infrastruktur[47] och genomförde under sommaren och hösten 2005 dessutom två seminarier med deltagande från medlemstaterna och, i det ena fallet, också från näringslivet. Syftet har varit att försöka ena EU:s institutioner och medlemsstater om mål och grundprinciper för ett sektorsövergripande europeiskt program för CIP (EPCIP) såsom gemensamma kriterier för att identifiera kritisk infrastruktur på nationell och europeisk nivå, miniminormer för skydd, nationella myndigheter för att överse arbetet etc. Kommissionen föreslog också inrättandet av ett ”critical infrastructure warning and information network” (CIWIN).

Tanken var att EPCIP skulle kunna beslutas före utgången av 2005 men svårigheterna att nå en gemensam ståndpunkt såväl inom EU:s institutioner som mellan medlemsstater visade sig allt för stora. Istället publicerade Kommissionen i november 2005 ett grönpapper[48] med syftet att få ”ytterligare återkoppling” avseende ett antal policyoptioner rörande EPCIP. Även om grönpappret formellt ställer ett antal frågor är det möjligt att ur hur dessa frågor är formulerade dra vissa slutsatser om vilka lösningar Kommissionen föredrar.[49] Eftersom det ännu inte finns några beslut om EPCIP:s innehåll måste emellertid det som skrivits och sagts inom ramen för denna process för tillfället tas som

[46] Council of the European Union: *Brussels European Council 17 and 18 June 2004 Presidency Conclusions*.
[47] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20. Commission of the European Union: *Preparedness and consequence management in the fight against terrorism*, COM(2004) 701, Brussels 2004-10-20. Commission of the European Union: *Prevention, preparedness and response to terrorist attacks*, COM(2004) 698, Brussels 2004-10-20.
[48] Ett grönpapper är i EU-terminologin ett pappers som ges ut för att stimulera till en öppen och bred diskussion kring en viss frågeställning som ett steg mot formulerandet av en EU-policy.
[49] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17. Grönpappret publicerades när föreliggande studie var i sitt absoluta slutskede. I möjligaste mån har dock i studien dock tagits hänsyn till grönpapprets innehåll. I huvudsak samlar emellertid meddelandet sådana frågeställningar som Kommissionen tidigare lagts fram i icke-officiella dokument, t.ex. i samband med seminarierna, varför studiens slutsatser endast i begränsad omfattning har påverkats av grönpappret.

indikationer. Att EU skall ta fram ett europeiskt program för skydd av kritisk infrastruktur, inklusive CIWIN, har dock Rådet beslutat i och med antagandet av Solidaritetsprogrammet.[50]

3.1.3 Skydd av kritisk infrastruktur i enskilda sakpolitikområden

Den tredje och sista nivån utgörs av EU:s arbete med frågor relaterade till skydd av kritisk infrastruktur i enskilda sakpolitikområden. Detta är inte något nytt. Inom vissa områden, som t.ex. informationssäkerhetsområdet, har detta pågått länge inte minst med hänvisning till den inre marknadens behov av ett enhetligt regelverk.[51]

Karaktären på samarbetet varierar från politikområde till politikområde. I vissa fall är det långtgående med omfattande regelverk och EU-ledda inspektioner av medlemsstaternas åtlydnad av direktiven. I andra fall handlar det om ramlag-stiftning inom vilken medlemsstaterna själva implementerar såväl nationell lag som inspektioner och sanktioner. Hittills tycks emellertid kopplingen mellan detta sedan länge pågående CIP-arbete och processen att ta fram en sektorsöver-gripande CIP-politik vara relativt svag – det är inte uppenbart ur materialet hur diskussionen om den sektorsövergripande politiken bygger på erfarenheterna från det sektorsspecifika samarbetet.

En beskrivning av CIP-arbetet i några sakpolitikområden återfinns i bilaga 2.

3.2 Vad utgör kritisk infrastruktur?

Kommissionen har föreslagit att kritisk infrastruktur skall definieras som

> Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States.[52]

---

[50] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01, sidan 12f.

[51] 1997 kom Europaparlamentet och Rådet med ett direktiv (97/33/EG) som fastslog ett regelverk för att inom gemenskapen säkerställa samtrafik mellan telenät och samverkan mellan tjänster. Bland så kallade "väsentliga krav" i direktivet kan nämnas att Medlemsstaterna skall kunna garantera upprätthållande av nätens integritet, dataskydd, etc. *Europaparlamentets och Rådets direktiv om samtrafik inom telekommunikationsområdet*, 97/33/EG, 1997-06-30.

[52] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20. Denna definition kan jämföras med Natos som lyder ”Critical Infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government.” Nato: *Critical Infrastructure Protection – Concept Paper*, EAPC(SCEPC)D2003)15, 2003-11-10. Bägge definitionerna är tämligen breda men fokuserar på tekniska facilititeter och system, inte på verksamheter

Inför det seminarium om CIP som Kommissionen genomförde i september 2005 utvecklades detta till att inrymma teknisk infrastruktur och nätverk, nyckelpersoner liksom styrprocesser för kritisk infrastruktur samt slutligen ”mjuka mål” med kulturellt eller politiskt värde, inklusive stora evenemang (sport, kultur etc.). Formuleringarna återkommer i Kommissionens grönpapper.[53]

Vid samma tillfälle presenterades Kommissionen också en indikativ lista över kritiska infrastruktursektorer, som sedan vidareutvecklades i grönpappret (se bilaga 1). För varje sektor presenteras en nedbruten lista över vilka kritiska produkter eller tjänster som infrastrukturerna inom sektorn levererade (energisektorn innehåller t.ex. produktion av olja, gas och elektricitet men också överföring och distribution av dessa produkter).

Kommissionen tycks således anlägga såväl system- som symbolperspektiv i definitionen av kritisk infrastruktur. Även om grunddefinitionen fokuserar på de konkreta, infrastrukturerna som sådana lägger den indikativa listan över infrastrukturer tonvikten på de tjänster och produkter som dessa levererar. Definitionerna nämner några vitala intressen (hälsa, säkerhet, fungerande stat etc.) men utan att det görs någon direkt koppling till de värden (frihet, demokrati, jämlikhet, rättsstatsprincipen etc.) som ingår i utkastet till nytt fördrag för EU.

Kommissionen har föreslagit att europeisk kritisk infrastruktur skall definieras som infrastruktur vars bortfall skulle få allvarliga konsekvenser för ”health, safety, security, economic or social well-being of two or more Member States”.[54] Definitionen har således en tonvikt mot medlemsstatsperspektivet (det är ekonomin, hälsosituationen, säkerheten etc. i medlemsstaterna som är utgångspunkten) och berör inte i direkt mening infrastruktur som stöttar värden eller vitala intressen på en europeisk nivå.[55] I vad mån en koppling är implicit antagen i definitionen är svårt att avgöra.

I denna definition ryms sådan infrastruktur som i sin konkreta uppbyggnad är transnationell (t.ex. distribution av elektricitet) men också sådan som är interdependent och vid avbrott skulle kunna generera effekter över EU:s inre gränser (t.ex. det finansiella systemet). Däremot är försäkringsperspektivet, d.v.s. infrastruktur där Unionen som helhet skulle vara ett rimligt försäkringskollektiv, inte tydligt i definitionen. Istället tycks det bara vara när de ekonomiska eller andra konsekvenserna av bortfall i en medlemsstat riskerar att sprida sig till andra medlemsstater som definitionen ser infrastrukturen som ”kritisk” på en europeisk nivå. Emellertid kan solidaritetsfonden bidra till en nyansering av

[53] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 20.
[54] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 20.
[55] Om inte denna ses som en indirekt följd av ekonomin i medlemsstaterna.

denna bild och ses som ett slags ”försäkring” som löser ut när en situation blivit sådan att det inte längre är rimligt att en enskild stat ensam har tillräckliga resurser.

Det kan också vara värt att notera att Kommissionens förslag till definition inte direkt pekar ut EU:s egna institutioner och strukturer som europeisk kritisk infrastruktur. Överlagras EU:s indikativa lista av punkter som t.ex. det finansiella systemet, administration samt lag och ordning på förslaget till definition av europeisk kritisk infrastruktur så bör emellertid åtminstone delar av EU-institutionerna, som t.ex. Europeiska centralbanken och EU:s interna informations- och kommunikationssystem kunna räknas in.

I sakpolitikområdena har det huvudsakliga argumentet för att identifiera en infrastruktur som att vara av europeiskt intresse varit i vilken mån den stödjer vissa europeiska vitala intressen, framförallt den inre marknaden och den fria konkurrensen, vilka i sin tur ses som förutsättningar för upprätthållandet av grundläggande värden. Detta gäller t.ex. för de transeuropeiska näten. En annan kategori är infrastrukturer för vilka EU som helhet utgör en rimlig varnings-, erfarenhets- och analysbas (livsmedelssäkerhet, skydd mot farliga ämnen). Transportsektorn, inte minst sjö- och lufttransporter, utgör slutligen exempel på infrastrukturer som blir ”europeisk” då ett gemensamt regelverk är nödvändigt för att åstadkomma ett heltäckande skydd – det räcker med en flygplats med dålig säkerhet för att ett hot skall kunna realiseras.

Kommissionen vill se en inom ett ”gemensamt ramverk” samordnad och harmoniserad analysprocess för arbetet med att identifiera kritisk infrastruktur, baserade på i EPCIP överenskomna, gemensamma kriterier. Även om Kommissionen i grönpappret formellt lämnar öppet för huruvida nationell kritisk infrastruktur skall utgöra en del av EPCIP, är det tydligt från formuleringarna att Kommissionen själv anser att så bör vara fallet.[56]

När det gäller nationell kritisk infrastruktur föreslår Kommissionen att medlemsstaterna själva skall ansvara för att ta fram de specifika kriterierna, inom ramen för det gemensamma ramverket, för identifiering av kritisk infrastruktur och sedan genomföra identifieringsarbetet. När det gäller europeisk kritisk infrastruktur är grönpapprets huvudlinje att Kommissionen tillsammans med medlemsstaterna skall utforma kriterier för identifieringen och genomföra identifieringsarbetet.[57] De av Kommissionen diskuterade uppifrån och ned – processerna för att identifiera nationell och europeisk kritisk infrastruktur innebär att

[56] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidorna 5 respektive 9.
[57] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidorna 8f samt 11ff.

detaljerad information kommer att lagras på medlemsstatsnivån vad gäller nationell kritisk infrastruktur och på EU-nivån vad gäller europeisk kritisk infrastruktur.

Grunden för identifieringsprocessen föreslås vara att värdera hur stor geografisk yta som skulle påverkas, vilka effekterna blir på allmänheten, ekonomin, miljön, politiska systemet och andra, beroende infrastrukturer samt hur tidsfaktorn påverkar när bortfall får allvarliga konsekvenser. Hur dessa kriterier skall tillämpas har inte närmare beskrivits.[58] Kopplingen till de värden som lyfts fram i utkastet till nytt fördrag är inte heller tydlig.[59]

När det gäller att identifiera europeisk kritisk infrastruktur föreslår Kommissionen att konsekvenserna värderas utifrån drabbad geografisk yta, påverkan över tid samt hur pass interdependent den aktuella infrastrukturen är med infrastruktur i andra medlemsstater.[60] Det andra kriteriet – tidskriteriet – innebär att analysen av konsekvenser inte avgränsas till det korta perspektivet av den omedelbara, akuta krisen. Kommissionens exemplifierar med ett radioaktivt molns utbredning över tiden. Detta kriterium skulle dock kunna leda till svåra avdömningar där enskilda medlemsstater inte nödvändigtvis alltid kommer att dela synen på vad som är ”europeiskt”. Innebär t.ex. tidskriteriet att det fysiska skyddet av Londonbörsen är en europeisk angelägenhet? En händelse som slår ut Londonbörsen skulle efter några dagar får omfattande konsekvenser för europeisk ekonomi.

Ägarna/operatörernas involvering i identifieringsprocessen är oklar och det nämns inte var i arbetet dessa eventuellt skall delta, utöver att de har en roll i att meddela när de uppfattar att deras infrastruktur faller inom ramen för det som av EU anses som kritisk. Däremot understryker Kommissionen i grönpappret i allmänna termer behovet av att involvera ägare/operatörer i ”partnerskap” och att på EU-nivån skapa forum för åsiktsutbyte.[61]

---

[58] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20, sidan 4f samt Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 21.

[59] Detta embryo till analysprocess är dock inte helt logiskt. Eftersom tidsfaktorn kan ha olika värde för t.ex. miljön och det politiska systemet borde även denna värderas individuellt för de olika värden som påverkas. Det hade också varit mer logiskt att lägga beroendekriteriet som en egen analysfaktor för att se vilka sekundära följdeffekter av ett bortfall som måste analyseras vidare. För en god uppställning av hur en systematisk och logisk analysprocess skulle kunna se ut se t.ex. Birgitta Lewerentz et al: *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system*, FOI MEMO 1283, mars 2005.

[60] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 20.

[61] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 12f.

Valet av mer specifika kriterier och hur processen där de nyttjas ser ut blir avgörande för vilka infrastrukturer som kommer att identifieras som ”kritiska” och om systemet är nedifrån och upp eller uppifrån och ned. Kommissionen verkar emellertid luta mot att EPCIP till största del skall vara obligatoriskt, vilket skulle innebära en generell uppifrån och ned karaktär åt identifieringen av kritisk infrastruktur.[62]

3.3 Mot vad skall kritisk infrastruktur skyddas?

I EU:s CIP-process har hittills inte gjorts någon tydlig åtskillnad mellan ”normala störningar” och större ingrepp såsom storskalig terrorism och naturkatastrofer. Den huvudsakliga drivkraften för EU:s arbete de senaste åren med sektorövergripande CIP har emellertid varit det hot som terrorismen uppfattats utgöra mot vitala resurser och strukturer. Detta gäller såväl processen på den övergripande politiska nivån, där såväl fördragsutkast och säkerhetsstrategi i stor utsträckning präglats av de senaste årens terrordåd, som i det konkreta arbetet med att ta fram ett europeiskt program för skydd av kritisk infrastruktur, EPCIP.

Emellertid har det CIP-relaterade arbetet inom specifika sakpolitikområden snarare drivits av de krav på funktionssäkerhet, informationssäkerhet och gemensamma spelregler som EU:s gemensamma marknad ställer. Det handlar om att skydda infrastrukturer av betydelse för marknadens funktion men också att tillse att regelverket för skydd av samhälle, egendom och liv utformas så att samma spelregler gäller för alla företag i hela EU. Därmed blir skyddet av infrastrukturen också mot mindre störningar en EU-fråga, åtminstone vad avser ”europeisk” infrastruktur.[63]

I den process som Kommissionen bedriver för att identifiera principerna för EPCIP verkar det nu växa fram en enighet kring all-hazards[64] men med ett särskilt fokus mot terrorism.[65] Solidaritetsklausulen i utkastet till nytt fördrag är i sig också ”all-hazards” till sin natur, då den betonar såväl terrorism som naturkatastrofer. Solidaritetsprogrammet har vidare som ett av sina strategiska mål att stärka förmågan till risk- och sårbarhetsanalyser inom EU och dess medlemsstater.[66] Kommissionen har också velat se att analys och värdering av

[62] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 6.
[63] Det gäller t.ex. inom IT-området där säkerhetsfrågorna understrukits i marknadsinitiativ som t.ex. eEurope. Se t.ex. Pär Eriksson: *Kartläggning av EU:s informationssäkerhetsarbete i första respektive andra pelaren*, FOI Memo1017, september 2004.
[64] D.v.s. att utöver terrorism även inkludera ett brett spektrum av andra hot (naturkatastrofer, olyckor etc.) i diskussionen.
[65] Lösningen med all-hazards men fokus mot terrorism kallas “flexibel” av Kommissionen. *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 3.
[66] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01, sidan 10.

risker skall ske på en ”harmoniserad” grund.[67] Sådana analyser kan knappast reduceras till att gälla någon eller några risker och hot utan analysen måste ske ”all-hazards” innan prioriteringar kan göras. Det innebär att även hotbilden som analyserna utgår från måste vara all-hazards.[68]

Solidaritetsprogrammet understryker att riskanalyser främst är en nationell uppgift.[69] I EPCIP-processen har Kommissionen betonat medlemsstaternas roll i att förse operatörer/ägare med relevant information om aktuell hotbild.[70] Emellertid efterlyser Solidaritetsprogrammet samtidigt att medlemsstaterna i arbetet med riskanalyser och förebyggande åtgärder bättre skall nyttiggöra de hotanalyser som t.ex. Rådets lägescentral (Situation Centre) och polissamarbetet EUROPOL genomför.[71]

På det utrikes- och säkerhetspolitiska området genomför Rådssekretariatets lägescentral underrättelseanalyser rörande stater och regioner, med hjälp av underrättelser från såväl EU:s institutioner som medlemsstaterna. Analysernas fokus beslutas bland annat utifrån den bevakningslista som medlemsstaterna arbetar fram i Kommittén för utrikes- och säkerhetspolitik (KUSP) och som fastställs av Rådet.[72]

Lägescentralen har dessutom redan idag i uppgift att genomföra analyser inom terrorismområdet, men exakt var och hur underrättelsebehoven formuleras är för denna studie oklart.[73] För CIP-området krävs det också en nivå som fastställer underrättelsebehov. I princip skulle PROCIV eller operativa kommittén kunna få en liknande roll som KUSP visavi lägescentralen. När det gäller EUROPOL, som är en myndighet, är detta samarbete av en annan karaktär och sker främst

---

[67] Commission: *Overview of initial ideas concerning the European Programme for Critical Infrastructure Protection*, opublicerat papper presenterat vid seminarium på Kommissionen 16-17 september 2005, sidan 4. Detta papper är inte ett officiellt kommissionsdokument och redovisar därmed inte nödvändigtvis Kommissionens samlade syn.

[68] Vilket inte är det samma som att de gemensamma åtgärderna inom EPCIP måste vara ”all-hazards”. Istället understryker Kommissionen ägare/operatörers ansvar för att hantera risker i anläggningar, distributionskedjor och informations- och kommunikationsnätverk.

[69] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01, sidan 10f.

[70] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20, sidan 9.

[71] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01, sidan 10f. EUROPOL har bl.a. till uppgift att samla in och sprida information om allvarliga brottstrender, inklusive terrorism. Det finns en särskild ”antiterroristgrupp” som främst syftar till informationsutbyte men som även genomför hotbildsanalyser. Se Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, sidan 44.

[72] I KUSP fastställs varje halvår den så kallade ”Global Watchlist” (på svenska bevakningslistan). I denna anges vilka stater och regioner som Unionen anser behöver följas upp underrättelsemässigt.

[73] Det som har sagts är bl.a. att lägescentralen har förmågan att, med hjälp av sekonderade nationella experter, analysera hotet från internationell terrorism. Analyserna stödjer arbetsgrupper och kommittéer. *http://www.homeoffice.gov.uk/about-us/eupresidency2005/presidency-priorities/eu-counter-terrorism/*

mellan medlemsstaternas polismyndigheter, och därmed svårare att inrikta via en kommitté. I den interrimslösning som upprättats för operativa kommittén ingår emellertid också en representant från EUROPOL varför det här redan finns en intressant koppling mellan kommittén och EUROPOLs arbete.

Slutligen diskuteras i Kommissionens grönpapper om EPCIP huruvida det föreslagna CIWIN (Critical Infrastructure Warning and Information Network) bör få en underrättelsebetonad roll att snabbt sprida information om omedelbara och aktuella hot. Mot detta står i diskussionen en uppfattning om ett mer begränsat mandat, att förmedla idéer och ”best practics”, på liknande vis som t.ex.”Major-Accident Reporting System” inom ramen för SEVESO II (se bilaga 2).[74] Det är emellertid oklart vad den förstnämnda rollen mer exakt skulle kunna innebära. Det finns visserligen varningsnätverk med en roll att snabbt förmedla hot inom t.ex. hälso- och informationssäkerhetsområdena. En uppblossande epidemi eller ett datavirus som sprider sig snabbt är dock en annan fråga än en enstaka utslagen infrastruktur. Även om det kan uppstå kaskadeffekter över medlemsstatsgränserna hanteras dessa då främst av de privata aktörerna som äger och/eller opererar infrastrukturerna.

3.4 Hur skall skyddet utformas?

Vid en analys av EU-diskussionerna avseende ett framtida unionsgemensamt, sektorsövergripande system för skydd av kritisk infrastruktur framtonar två olika, men inte nödvändigt helt ömsesidigt uteslutande, bilder. Den första är bilden av ett tämligen centraliserat system där EU har en styrande och normerande roll. Kärnan utgörs av det europeiska programmet för skydd av kritisk infrastruktur (EPCIP) som det diskuteras i Kommissionens grönpapper.[75]

Den andra är bilden av ett system i huvudsak inriktat på att stödja samverkan, koordination, kunskapsbyggande och kunskapsutbyte mellan medlemsstater och mellan medlemstater och EU-institutioner. Denna bild framträder tydligast i de politiska handlingsprogram och strategier som Rådet har beslutat (Haagprogrammet, Handlingsplanen för terrorismbekämpning, Solidaritetsprogrammet etc.).

EPCIP:s målsättning föreslås i Kommissionens grönpapper vara att inom EU säkra tillräckliga och lika skyddsnivåer för kritisk infrastruktur, så få och ofarliga avbrott som möjligt samt snabba arrangemang för återställande infrastruktur. För att skapa dessa tillräckliga och lika skyddsnivåer, och

[74] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 14.
[75] Grönpappret är ett diskussionsunderlag, inte ett formellt kommissionsförslag. Kommissionen lyfter i pappret fram ett antal frågeställningar som den anser behöver dömas av. Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17.

samtidigt undvika att störa den inre marknaden, förespråkar Kommissionen i grönpappret ett ”gemensamt ramverk”. Detta ramverk föreslås ha såväl en horisontell dimension (regelverk gällande alla sektorer, t.ex. vad gäller ägare/operatörers skyldigheter och rättigheter) som en vertikal dimension (sektorsspecifika regelverk, t.ex. rörande skyddsnivåer).[76]

I detta ramverk fastställs kriterier för identifiering av europeisk respektive nationell kritisk infrastruktur vilka sedan utnyttjas för sektorsvisa analyser. Därefter analyseras eventuella säkerhetsbrister i utpekad kritisk infrastruktur, som en grund för att avgöra vilka sektorer och infrastrukturer som är prioriterade. Slutligen föreslås i grönpappret att det för varje sektor skall utvecklas miniminivåer för skyddet, som sedan implementeras och övervakas.[77]

I Solidaritetsprogrammet sägs att Kommissionen ”skall fokusera på infrastrukturer med transnationella effekter, övriga skall förbli helt under medlemsstaternas ansvar inom ett gemensamt ramverk”.[78] I Kommissionens grönpapper ges EU en stor roll när det gäller att identifiera och analysera europeisk kritisk infrastruktur (Kommissionen tillsammans med medlemsstaterna) men också i att fastställa miniminivåer för skyddet (Rådet) och i att följa upp dessa skyddsnivåers implementering (Kommissionen tillsammans med medlemsstaterna).[79]

När det gäller nationell kritisk infrastruktur lämnar Kommissionen i grönpappret formellt frågan öppen huruvida denna skall omfattas av EPCIP, men det är ändå tydligt utifrån skrivningarna att Kommission anser att så bör vara fallet.[80] För nationell kritisk infrastruktur föreslår Kommissionen i grönpappret samma analys- och implementeringssteg som för europeisk, med den skillnaden att för nationell infrastruktur är det medlemsstaterna som skall driva processerna ”med utgångspunkt från EPCIPs gemensamma ramverk”.[81]

Kommissionen menar vidare i grönpappret att ”effektiviteten” kräver en organisation med nationella, EPCIP-ansvariga myndigheter som skall fungera som dels nationell kontaktpunkt för EPCIP-programmet, dels nationellt ansvarig myndighet för implementeringen av EPCIP. Denna myndighet skall, enligt grönpappret, kunna delta i utpekandet av europeisk nationell infrastruktur och

[76] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 3 och 5.
[77] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 7ff.
[78] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01.
[79] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 8.
[80] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 9.
[81] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 9ff

ansvara för nationella beslut att utpeka nationell kritisk infrastruktur. Vidare föreslås myndigheten delta i utvecklandet av nationella skyddsprogram för kritisk infrastruktur och identifiera beroenden mellan olika sektorer. Slutligen föreslår Kommissionen också att denna nationella EPCIP-myndighet skall bidra till sektorsspecifika förhållningssätt till CIP, där även ägare/operatörer kan delta i diskussionerna, samt övervaka upprättandet av omfallsplaner rörande kritisk infrastruktur.[82]

Det är svårt att ur grönpappret utläsa exakt vilket inflytande EU, med ett EPCIP som Kommissionen skissar det, i praktiken skulle få över sådant som pekats ut som nationell kritisk infrastruktur. Dock kan konstateras att det ”gemensamma ramverket” som skall utgöra ”utgångspunkt” för medlemsstaternas arbete, tillsammans med det uppifrån och ned system med nationella EPCIP-myndigheter som Kommissionen lyfter fram, får EPCIP en styrande roll även för medlemsstaternas kriterier och analyser rörande nationell kritisk infrastruktur. Kommissionen påpekar också särskilt att beroenden mellan infrastrukturer understryker behovet av ett mer allomfattande ramverk samt noterar att säkerhetssystem måste vara konsistenta och logiska även mellan sektorer.[83]

Inom vissa sakpolitikområden, som t.ex. skydd mot kemolyckor, finns redan ett formaliserat europeiskt inflytande, inklusive inspektioner, av infrastrukturer. För andra områden, t.ex. kontroll av dricksvatten, finns detaljerade EU-direktiv men det är medlemsstaterna som står för implementering och uppföljning. Kommissionen tycks i grönpappret förespråka att EPCIP skall ha ett legalt ramverk, troligen i form av ett ramdirektiv som sätter upp målsättningar men lämnar öppet för medlemsstaterna själva att besluta om den närmare implementering i nationell lagstiftning. Vilka delar av EPCIP som skulle ingå i ett sådant ramdirektiv och mer exakt på vilket sätt framgår dock inte.[84]

Kommissionen har inom ramen för EPCIP-processen också angivit en roll för EU i samverkan med privata operatörer och ägare av infrastruktur. EPCIP skall enligt Kommissionen bidra till att skapa partnerskap mellan berörda aktörer, privata och offentliga, för att dela information relaterad till kritisk infrastruktur.[85] Samverkan för koordination och samarbete skall enligt förslagen upprättas på nationell och europeisk nivå mellan ägare/operatörer,

---

[82] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 10f.
[83] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 5 och 9.
[84] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 6.
[85] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20, sidan 8f.

branschorganisationer, statsmakten och allmänheten.[86] Kommissionen förespråkar, som nämnts ovan, också att EPCIP vid behov skall kunna stödja framväxten av europeiska industriföreningar rörande CIP-frågor.

Varje nationell och europeisk kritisk infrastruktur bör enligt Kommissionen utse en särskild befattningshavare (”security liaison officer”) för att samverka med nationell, sektorsövergripande EPCIP-myndighet. Varje nationell och europeisk kritisk infrastruktur skall dessutom utveckla en säkerhetsplan (”operator security plan”), där såväl infrastruktur som åtgärder till skydd för denna skall ingå, vilken skall godkännas av relevant ”sektorsansvarig myndighet under översikt av nationell EPCIP-myndighet”. De skyddsåtgärder som vidtas kan vara permanenta eller sådana som sätts in i situationer av ökat hot. Dessutom skall infrastrukturens ägare/operatör också delta i utvecklingen av omfallsplaner tillsammans med bl.a. nationella räddningstjänst- och rättsmyndigheter.[87]

Ägare och operatörer skall samtidigt via nationell EPCIP-myndighet, men också via nationella rättsvårdande myndigheter och när lämpligt via Kommissionen, få tillgång till råd och information rörande skydd och säkerhet (som t.ex. best practices), säkerhetsstrategier för att möta terrorism samt aktuella hot.[88] Medlemsstaterna skall också stödja ägare och operatörer med utveckling och revision av beredskaps- och säkerhetsplaner.

För att hantera ett EPCIP krävs på EU-nivån att ett sektorsövergripande organ pekas ut som ansvarig för den politiska inriktningen av EPCIP-processen under Rådet. Civil Protection Working Party (PROCIV, en rådsarbetsgrupp under COREPER) har för tillfället en sådan roll men behöver då utformas och mötas i sådana konstellationer som är relevanta för detta ändamål. Det samma gäller om frågan i framtiden i stället skulle läggas på den operativa kommittén. Här finns också en koppling till utvecklingen av ARGUS och Haagprogrammets ”integrerade krishanteringsarrangemang”.

Det krävs inom EU-strukturen också ett beredande organ för att förbereda och utveckla politiken, för att utveckla regelverk och för att samordna och utveckla av kunskap om sak och metod. Hur ett sådant beredande organ inom Kommis-

[86] Commission of the European Union: *Overview of initial ideas concerning the European Programme for Critical Infrastructure Protection*, opublicerat papper presenterat vid seminarium på Kommissionen 16-17 september 2005, sidan 3. Detta papper utgör emellertid inte ett officiellt Kommissionsdokument och redovisar därför inte nödvändigtvis Kommissionens samlade syn.
[87] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 12f.
[88] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 12f samt Commission of the European Union: *Overview of initial ideas concerning the European Programme for Critical Infrastructure Protection*, opublicerat papper presenterat vid seminarium på Kommissionen 16-17 september 2005, sidan 3. Detta papper utgör emellertid inte ett officiellt Kommissionsdokument och redovisar därför inte nödvändigtvis Kommissionens samlade syn.

sionen skulle förhålla sig till övriga delar av Kommissionen, där sakpolitiken formas, är ännu oklart. För närvarande är det direktoratet för Frihet, rättvisa och säkerhet som driver processen men det är inte otroligt att det inom Kommissionen finns olika syn såväl på vem som skall ha denna roll som hur långtgående den skall vara. När det gäller mer analyserande uppgifter kan Joint Research Centre (JRC) få en roll på samma sätt som det t.ex. fått för att hålla samman analys av olyckor med farliga ämnen. I Kommissionens förslag till specifikt program för JRC under det sjunde ramprogrammet ingår också att ge stöd till värdera hot och sårbarheter för kritisk infrastruktur ”på unionsnivå” och förebyggandet av angrepp mot infrastrukturer.[89]

Den andra, delvis alternativa, rollen för EU avseende CIP som framträder vid en analys av EU-processerna är att stödja koordination, samordning och utveckling av en gemensam uppfattning om vad som utgör kritisk infrastruktur, hur hotet ser ut samt hur hot, risker och sårbarheter analyseras och värderas etc. Detta kan ske genom gemensamt utvecklings- och forskningsarbete men också genom ökat utbyte av erfarenheter och kunskap. Denna roll framträder klarast i de handlingsprogram och strategier som Rådet lagt fram.

Solidaritetsprogrammet talar t.ex. om att stimulera till ökad samverkan mellan olika nationella myndigheter involverade i riskanalyser om såväl sak som metod men också medlemsstaternas koordination och samarbete, när nödvändigt, rörande skyddsfrågor. Solidaritetsprogrammet understryker behovet av ett EPCIP, inklusive CIWIN, men även om man inte utesluter horisontella, koordinerande åtgärder på EU-nivå så tycks tyngdpunkten ligga på koordinering, samverkan och informationsutbyte snarare än en styrande, normgivande process.[90] CIWIN, tolkat som ett forum för informationsutbyte, skulle med denna tyngdpunkt kunna få en central roll i samverkan rörande analyser, metoder och ”best practices” inom CIP.

Ramprogrammet för säkerhet och skydd av friheter syftar bl.a till att stimulera och stödja risk- och hotanalyser och att öka medlemsstaternas förmåga såväl i det direkta arbetet med att skydda infrastrukturer som i arbetet att stödja operatörer och ägare i skyddet av infrastrukturer. Särskild prioritet ges till projekt som skapar strukturer och koordineringsmekanismer som är transnationella.[91] I sakpolitikområden återfinns också redan idag utbyte av ”best practices” och information som centrala delar.

---

[89] Commission of the European Union: *Proposal for a Council decision concerning the Specific Programme to be carried out by means of direct actions by the Joint Research Centre*, COM(2005)439, 2005-09-21, sidan 29.
[90] Council of the European Union: *EU Solidarity Programme on the consequences of terrorist threats and attacks*, 15480/04, 2004-12-01, sidan 10ff.
[91] Commission of the European Communities: *Communication from the Commission to the Council and the European Parliament Establishing a framework programme on “Security and Safeguarding Liberties” for the period 2007-2013*, COM(2005)124 Final, 2005-04-06, sidan 22f.

Även EU:s säkerhetsforskningsprogram, vilket blir en del av det kommande sjunde ramforskningsprogrammet, kan få en central roll i att utveckla en gemensam kunskap och att ensa synsätt. Redan i de förberedande forskningsomgångarna har flera projekt rörande skydd av kritisk infrastruktur initierats. Ett är VITA (”Vital Infrastructure Threats and Assurance”) som syftar till att finna metoder och verktyg för att analysera och skydda infrastrukturer i nätverk och ett annat är PATIN som syftar till att studera hur skyddet kan förbättras för hela lufttransportsystemet.[92] Emellertid bör understrykas att säkerhetsforskning redan tidigare genomförts inom ramen för olika Generaldirektorats verksamhet, inte minst inom informationsteknikområdet.

Det är i de nuvarande diskussionerna inte aktuellt är att ge EU en operativ roll i skyddet av kritisk infrastruktur t.ex. avseende återställande eller ersättande av infrastruktur. Kommissionen har inte heller i de nuvarande processerna sökt någon sådan roll. Inte heller i enskilda sakpolitikområden har EU denna typ av roll. Om insatser av en mer operativ karaktär blir aktuella, t.ex. för att ersätta viss infrastruktur, sker dessa med resurser från medlemsstaterna, under ledning av en eller flera medlemsstater, möjligen koordinerade av EU i form av t.ex. resursregister.

När det gäller finansieringsfrågorna betonar Kommissionen i sitt meddelande från 2004 såväl att samhället måste bära de kostnader för skydd som beror av hot mot hela samhället som att operatörer har stort eget ansvar för att skydda sin verksamhet.[93] Det EU i nuläget är beredd att finansiera på en sektorsövergripande CIP-nivå är åtgärder för att identifiera och analysera risker och sårbarheter, men också åtgärder för att generellt öka förmågan hos medlemsstater och aktörer att hantera skyddet av kritisk infrastruktur samt utveckling av former och arrangemang för samarbete.[94] Däremot tycks det vara mindre sannolikt med finansiering av konkreta skyddsåtgärder som redundanskapacitet eller utökat fysiskt skydd. Detta kan dock i någon mån komma att ske inom de olika sakpolitikområdena såsom t.ex. Kommissionen föreslagit inom ramen för utvecklingen av de transeuropeiska nätverken (se bilaga 2).

[92] Mer information om säkerhetsforskningsprogrammet finns på www.cordis.lu.
[93] Man betonar bl.a. att operatörer och ägare av infrastruktur har det främsta ansvaret för att hantera risker i anläggningar, distributionskedjor, informationsteknologi och kommunikationsnätverk. Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20, sidan 4f.
[94] Commission of the European Communities: *Communication from the Commission to the Council and the European Parliament Establishing a framework programme on “Security and Safeguarding Liberties” for the period 2007-2013*, COM(2005)124 Final, 2005-04-06, sidan 22f.

4 Sverige och skydd av kritisk infrastruktur

4.1 Allmänt om den svenska krisberedskapsprocessen

I detta kapitel beskrivs först det allmänna svenska systemet för krisberedskap för att sedan gå in på diskussioner specifika för de tidigare identifierade jämförelsefaktorerna.

4.1.1 Sveriges krisberedskapssystem

Under det kalla kriget var skyddet av kritisk infrastruktur en central del av Sveriges civilförsvar – samhällets förmåga att stödja krigsinsatsen fick inte vara möjlig att lamslå. En del av skyddet var också att hålla Sverige oberoende antingen genom en egen produktion av centrala produkter eller genom beredskapslagring. Denna aspekt avfördes i princip helt från agendan efter det kalla krigets slut då också de flesta beredskapslager successivt avvecklades. Under nittiotalet kom istället kraven från ett ökat internationellt engagemang att dominera diskussionerna.

I slutet av nittiotalet återvann infrastrukturfrågorna successivt vikt. Fokus låg nu på de sårbarheter som byggts in i samhället, inte minst genom utvecklingen på informationsteknikområdet. Försvarsberedningen genomförde i sina rapporter från 2001[95] för första gången en fördjupad diskussion kring IT-hotet. Parallellt presenterade Sårbarhets- och säkerhetsutredningen sitt betänkande[96] som bl.a. diskuterade såväl hot- och sårbarhetsutveckling som samhällets krishanterings syfte och struktur.

Rapporten kom att ligga till grund för den proposition om det civila krishanteringssystemet som regeringen presenterade våren 2002.[97] Som direkt följd av denna antogs en serie lagar som styr det svenska beredskapsarbetet.[98] Denna utgör också den senaste genomgripande förändringen av det övergripande svenska krishanteringssystemet.[99] Våren 2006 förväntas emellertid en ny proposition, som bland annat bygger på erfarenheterna från det nuvarande systemet, på utredningen kring Tsunamihanteringen, på utredningen kring militärt stöd till civil krishantering och på informationssäkerhetsutredningen. Här föreliggande studie kommer emellertid att utgå från dagens system.

---

[95] Försvarsberedningen: *Gränsöverskridande sårbarhet – Gemensam säkerhet*, DS 2001:14 samt Försvarsberedningen: *Ny struktur för ökad säkerhet – nätverksförsvar och krishantering*, DS 2001:44.
[96] Sårbarhets- och säkerhetsutredningen: *Säkerhet i en ny tid*, SOU 2001:14.
[97] Regeringen: *Samhällets säkerhet och beredskap*, proposition 2001/02:158, 2002-03-14.
[98] En kortfattad beskrivning av dessa lagar återfinnes i bilaga 3.
[99] Det har dock genomförts ett antal mindre, men viktiga, förändringar framförallt på IT-området, t.ex. införandet av en svensk CERT-funktion.

Det krishanteringssystem som inrättades i och med 2002 års proposition om det civila krishanteringssystemet innebar att ett system med geografiskt områdesansvar och samverkansansvar infördes och ersatte det tidigare funktionsansvaret. Myndigheters sektorsansvar kvarstod men skall stödjas av samordningsansvariga på olika geografiska nivåer (kommun, länsstyrelse, regering) vilka skall bidra till inriktning, prioritering av resurser och identifiering av tvärsektoriella åtgärder.[100]

Krisberedskapsmyndighetens roll är bl.a. att verka för samordning av planeringssystemet avseende svåra påfrestningar och det civila försvaret, att utveckla och förvalta principer för samverkansformer mellan offentlig sektor och näringsliv och att svara för analyser av samhällsutveckling, omvärldsförhållanden, beroendeförhållanden mellan viktiga samhällsfunktioner och deras sårbarheter. Krisberedskapsmyndigheten skall också lämna förslag till regeringen om fördelning av resurser för civilt försvar och åtgärder som stärker beredskapen mot svåra påfrestningar på samhället i fred och dessutom fördela resurser för sådana åtgärder till de olika myndigheter som skall bedriva verksamhet inom de olika så kallade samverkansområdena (se nedan).[101]

Ett centralt begrepp i det svenska krisberedskapssystemet är underifrånperspektivet som inbegriper dels principerna om ansvar (i möjligaste mån skall samma myndigheter ha ansvaret såväl i normalläge som i kris), likhet (samma organisation i fred, kris och krig) och närhet (hantera kriserna på en så nära/låg nivå som möjligt), dels att samhällets förmåga att hantera ”normala” kriser skall utgöra grunden för att hantera svåra påfrestningar.[102]

Det svenska krisberedskapssystemet är tämligen distribuerat och decentraliserat. Kommuner och myndigheter har centrala men självständiga roller, något som accentueras av det kommunala självstyret och den svenska modellen med självständiga myndigheter under regeringen. Krisberedskapsmyndighetens roll utövas dels genom att stödja samordningen av myndigheterna, dels genom ansvaret för att driva planeringsprocessen.

Ett antal myndigheter har tilldelats ett särskilt sektorsansvar (de så kallade samverkansmyndigheterna) och delats in i sex samverkansområden:

- Teknisk infrastruktur,
- Transporter,

[100] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, sidan 24ff.
[101] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, passim
[102] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, sidan 27.

- Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen,
- Ekonomisk säkerhet,
- Områdesvis samordning, samverkan och information (där även länsstyrelserna ingår),
- Skydd, undsättning och vård.

Syftet med samverkansområden är att samordna åtgärder som berör flera myndigheter men samtidigt också, enligt KBM, att tillse att myndigheterna tar en större del av ansvaret för samverkan själva.[103]

Indelningen i samverkansområden kan kritiseras för att vara en lista av ”äpplen och päron”. Medan rubriken ”ekonomisk säkerhet” beskriver ett övergripande samhällsvärde, beskriver rubriken ”teknisk infrastruktur” närmast system och rubriken ”Skydd, undsättning och vård” tjänster. En ytterligare risk med indelningen är att den inte på ett bra vis tydliggör att i dag är i princip alla tjänster beroende av såväl tekniska system, personal och ledningsförmåga.[104]

4.2 Vad utgör kritisk infrastruktur?

Det allmänna systemet för hanterande av fredstida kriser och situationer av höjd beredskap är inte detsamma som det mer specifika skyddet av kritisk, eller som det benämns i Sverige, samhällsviktig infrastruktur. Samverkansområdena är bredare än bara skydd av sådan infrastruktur. I dessa ligger också försörjnings-säkerhet, krisinformation, krishantering/konsekvenshantering etc. vilka visserligen är centrala i hanteringen av en kris men som inte nödvändigtvis tillhör skyddet av kritisk infrastruktur.

I Sverige ligger fokus på vad som brukar kallas ”samhällsviktig verksamhet” snarare än på tekniska infrastrukturer i sig. De infrastrukturer som krävs för att genomföra denna verksamhet blir indirekt utpekade som ”samhällsviktiga”. En samhällsviktig verksamhet kan typiskt stödjas av flera samhällsviktiga

[103] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, sidan 82. KBM har lagt förslag om framtida inriktning av systemet. Bland annat vill KBM se en tydligare beskrivning av länsstyrelsernas geografiska samordningsuppdrag samtidigt som länsstyrelserna ges en tydligare roll i alla samverkansområden för att på så vis uppnå en bättre integration mellan sektors- och geografiskt områdesansvar. Det särskilda samverkansområdet för ”områdesvis samordning, samverkan och information” skulle då helt inriktas på aspekter av den geografiska samordningen. Krisberedskapsmyndigheten föreslår också införandet av en ny kategori för myndigheter involverade i krisberedskapen – stödmyndigheter – som kan vara centrala för samhällets krishanteringsförmåga men vars kompetens är sektorsövergripande eller endast i vissa typer av kriser efterfrågad. KBM vill slutligen också se en tydligare roll för sig själv i att stödja och samrodna arbetet, inklusive att uppmärksamma frågor av övergripande karaktär, i samtliga samverkansområden. Se ”En ny krisberedskapsförordning”, i Krisberedskapsmyndigheten: *Så vill vi utveckla krisberedskapen*, KBM 2005, sidan 147 ff.

[104] Samtal Jan Lundberg, Krisberedskapsmyndigheten, juni 2005.

infrastrukturer samtidigt som en infrastruktur typiskt stödjer flera verksamheter.[105] Vad som utgör samhällsviktig verksamhet är emellertid inte särskilt väldefinierat. Krisberedskapsmyndigheten har för närvarande ett regeringsuppdrag att arbeta fram en definition av vad som utgör samhällsviktig verksamhet.[106] En allmän bild av vad samhällsviktig verksamhet är skulle kunna vara verksamheter som är nödvändiga för att i en kris säkra för samhället vitala intressen (som t.ex. upprätthålla en demokratisk rättsstat) som i sin tur är nödvändiga för att upprätthålla grundläggande värden (som t.ex. demokrati och rättsstatsprincipen).

I inriktningsdokumentet inför 2007 ger KBM en lite mer konkret bild av vad man uppfattar utgör samhällsviktig infrastruktur:[107]

> Med samhällsviktig infrastruktur avses bland annat elförsörjningen, telekommunikationerna, vissa IT-system och distributionen av radio- och TV-program. Hit kan också räknas kommunaltekniska försörjningssystem som VA-system och fjärrvärme. Till de samhällsviktiga transportsystemen räknas vissa persontransport-, godstransport- och varudistributionssystem. Även vissa finansiella system måste klassas som del av den samhällsviktiga infrastrukturen. Hit hör bland annat betalningssystemet och socialförsäkringssystemen.

Sammantaget tycks Sverige i huvudsak, för att använda Jan Metzgers terminologi, ha ett systemperspektiv. Det är systemets roll för andra system eller för samhällsviktiga verksamheter som avgör huruvida den är kritisk eller ej. Krisberedskapsmyndighetens beskrivning av kritisk infrastruktur är deskriptiv, utan några kriterier angivna för urval och utan att ta sin utgångspunkt i några värden eller samhällsintressen. Det är dock troligt att det pågående arbetet med att ta fram en mer utvecklad definition av samhällsviktig verksamhet, och därmed också indirekt samhällskritisk infrastruktur, för att bli konsistent behöver koppla till diskussionen om vad som utgör samhällsvärden.

Det finns inte någon utvecklad svensk, officiell uppfattning om vad som bör anses som transnationell infrastruktur i allmänhet eller europeisk kritisk infrastruktur i synnerhet. Däremot har såväl regeringen som Krisberedskapsmyndigheten i generella termer understrukit infrastrukturens internationalisering och det därav följande behovet av fördjupat samarbete. Inom sakpolitikområden, som SEVESO, flygsäkerhet, vattensäkerhet, livsmedelssäkerhet, informationssäkerhet etc. deltar Sverige också i CIP-relaterade processer med varierande grad av EU-inflytande.

---

[105] Peter Stern, Krisberedskapsmyndigheten, vid projektseminarium på KBM 2005-09-30.
[106] Krisberedskapsmyndigheten, diarienummer 0253/2005.
[107] Krisberedskapsmyndigheten: *Samhällets krisberedskap. Inriktning av verksamheten 2007*, KBM Planeringsprocessen 2005:03, sidan 27.

Sverige tycks således snarast tveka inför en generell sektorsövergripande roll för EU. I diskussioner om EU:s roll har Sverige dessutom betonat EU:s mervärde som kanal för informations- och erfarenhetsutbyte, snarare än som sektorsövergripande organ för ”gemensam” infrastruktur (se avsnitt 4.4). Slutligen har Sverige hittills menat att infrastrukturer som sträcker sig över endast två medlemsstater skall betraktas som bilaterala, inte europeiska, och ansett att det mervärde EU-nivån kan tillföra dessa är begränsat.

Det svenska krisberedskapssystemets allmänna planeringsprocess är i mångt och mycket en förhandlingsprocess där Krisberedskapsmyndigheten tillsammans med samverkansmyndigheter arbetar sig fram till målsättningar och prioriteringar. I planeringsinriktningen ges bl.a. övergripande målsättningar för de olika samverkansområdenas arbete tillsammans med en planeringsram.

De övergripande målsättningarna tas fram ”av KBM i samverkan med myndigheterna”.[108] Samtidigt skall inriktningen bygga på ”en konkretisering av riksdagens och regeringens övergripande plan för säkerhets- och försvarspolitiken” tillsammans med den årliga uppföljning som KBM genomför av krisberedskapen, de fördjupade genomgångar KBM genomför inom utvalda områden samt myndigheternas risk- och sårbarhetsanalyser.[109]

Utifrån en fortsatt process, där myndigheterna var för sig och inom respektive samverkansområde överväger ”vilka åtgärder som bör vidtas för att minska sårbarheten och öka säkerheten” och lämnar underlag till KBM, genomför KBM en dialog med alla myndigheter och lämnar ett samlat planeringsunderlag till regeringen. Sektorsmyndigheterna har ansvar för kontakterna med ägare/-operatörer. Krisberedskapsmyndigheten genomför också årliga utvärderingar av vidtagna åtgärder.[110]

Det svenska förhandlingssystemet innebär således en hierarki av målsättningar. Medan Krisberedskapsmyndigheten kan konstatera att en viss funktion är särskilt viktig men har ett otillräckligt skydd, är det den ansvariga myndigheten som i samverkansområdet anger vilka skyddsinsatser som bör prioriteras.[111] Samtidigt ligger mycket av tyngden i processen hos de enskilda myndigheterna och i de enskilda samverkansområdena, varför karaktären ändå blir ”nedifrån och upp”.

---

[108] Krisberedskapsmyndigheten: *Samhällets krisberedskap. Inriktning av verksamheten 2007*, KBM Planeringsprocessen 2005:03, sidan 30.
[109] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, sidan 81f.
[110] Krisberedskapsmyndigheten: *Förebygga och förbereda – så fungerar samhällets beredskap*, KBM 2005, sidan 82.
[111] Peter Stern, Krisberedskapsmyndigheten, vid projektseminarium på KBM 2005-09-30.

Det finns en styrka i det svenska systemets betoning av att beslut och prioriteringar så långt som möjligt skall baseras på bedömningar från dem som är nära den faktiska verksamheten. Samtidigt torde ett distribuerat system som det svenska ställa höga krav på den sammanhållande funktionen för att undvika felprioriteringar (ett samverkansområde lägst prioriterade åtgärd får ingen finansiering medan ett annat områdes högst prioriterade åtgärd får full finansiering trots att den är mindre viktig totalt sett) och suboptimeringar (åtgärder som görs i olika områden stöder inte varandra mot ett sammantaget säkrare samhälle).

Det är sammantaget svårt att i det svenska systemet identifiera en specifik och konkret lista över kritisk infrastruktur eller en analysprocess med tydliga kriterier för att ta fram en sådan lista. Ett skäl till detta kan vara att ett förhandlingsbaserat system som det svenska har svårt att hantera mer strukturerade, sektorsövergripande analyser för att identifiera de största behoven. Krisberedskapsmyndighetens pågående arbete med att utveckla en definition av ”samhällsviktig verksamhet” kan möjligen vara ett steg på vägen mot en konkretisering.

Vad som i en svensk kontext menas med ”kritisk infrastruktur” skulle möjligen också kunna identifieras ”bakvägen”, genom att se till vilka typer av projekt inom samverkansområdena som pengar allokeras. En sådan genomgång ligger emellertid utanför här föreliggande studies ram.

4.3 Mot vad skall kritisk infrastruktur skyddas?

Krisberedskapsmyndigheten ger sedan 2004 årligen ut en hot- och riskrapport, som syftar till att fungera ”som ett ingångsvärde för myndigheternas årliga risk- och sårbarhetsanalyser”. I denna diskuteras både aktörsbundna och icke aktörsbundna hot. Rapporten bygger bl.a. på KBM:s egen omvärldsanalys och på sektorsvisa hot- och riskanalyser. Denna hotanalys arbetas sedan in i inriktningsdokumentet för samhällets krisberedskap. Myndigheterna får därmed hjälp med en hotbild. Denna är emellertid inte normerande utan myndigheterna avgör själva vilken hotbild de skall arbeta utifrån. På så vis kan detta sägas vara såväl uppifrån och ned som nedifrån och upp.[112]

Myndigheter och även infrastrukturägare kan samtidigt få hjälp med hotbild även direkt från säkerhetstjänsten. Därmed får i Sverige även SÄPO en roll, utöver den KBM tar på sig i inriktningsdokumentet.

Sverige skiljer mellan ”normala störningar” och hot som kan leda till svåra påfrestningar för samhället. Definitionen av svåra påfrestningar är dock vag. I propositionen ”Samhällets säkerhet och beredskap” från 2002 anges att:[113]

[112] Krisberedskapsmyndigheten: *Hot- och riskrapport 2004*, KBM:s temaserie 2004:6.
[113] Regeringen: *Samhällets säkerhet och beredskap*, proposition 2001/02:158, 2002-03-14, sidan 25.

> en svår påfrestning inte är en enskild händelse i sig, exempelvis en olycka, ett sabotage osv., utan ett tillstånd som kan uppstå när en eller flera händelser utvecklar sig eller eskalerar till att omfatta flera delar av samhället. Svåra påfrestningar kan sägas utgöra olika slag av extrema situationer med låg sannolikhet som skiljer sig åt i sak. Tillståndet är av en sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen och därmed begränsa konsekvenserna.

Samtidigt påpekas i propositionstexten att det vare sig är möjligt eller önskvärt att exakt definiera vad som utgör en svår påfrestning. Samhället skall dessutom ha förmåga att hantera alla händelser i fred, oavsett om den utgör en mer begränsad störning eller om den kan leda till en svår påfrestning. För en myndighet eller operatör innebär detta att de skall ha förmåga att möta såväl de normala störningarna som extraordinära händelser med i princip samma resurser och organisation.

Begreppet svåra påfrestningar, som det är definierat, handlar således om omfattande och komplexa händelseförlopp. Av moderna svenska kriser är det troligen bara stormen Gudrun som skulle kunna anses som en svår påfrestning, då på regional nivå. Händelser som Madrid- eller London-dåden skulle däremot troligen inte räknas som svåra påfrestningar då deras effekter i tiden var relativt korta.

Sverige har sammantaget ett synsätt som är ”all-hazards” avseende hotet. Samhället skall ha förmåga att hantera såväl aktörsstyrda hot som icke-aktörsstyrda, såväl små störningar som stora kriser, med i princip samma organisation och resurser.

4.4 Hur skall skyddet utformas?

I Sverige har varje myndighet, organisation och företag var för sig huvudansvaret för att skydda sina anläggningar och verksamheten inom sitt ansvarsområde. Både ansvarsprincipen och planeringsprocessen (se avsnitt 4.1) pekar mot ett i grunden nedifrån och upp perspektiv i hanteringen av skyddet. I en faktisk krissituation är det de geografiska samordningsmyndigheterna på lokal (kommun), regional (länsstyrelse) och nationell (regering) nivå som ansvarar för prioritering av resurser och inriktning av insatser i det akuta skedet t.ex. för återställande eller ersättande av infrastruktur. Systemet är således i grunden decentraliserat. Krisberedskapsmyndigheten har en samordnade, sektorsövergripande roll i planeringsarbetet och leder dessutom en process för att allokera medel för det långsiktiga uppbyggandet av skyddet. Krisberedskapsmyndigheten har däremot inte någon operativ roll i en faktisk krissituation, utöver vid behov expertstöd till myndigheter samt lägesinformation till regeringen.

Krisberedskapsmyndigheten talar om två nivåer i beredskapsarbetet: grundsäkerhet och förstärkt förmåga. Grundsäkerhet utgörs av förmågan att hantera störningar med ordinarie organisation och resurser. Den förstärkta förmågan innebär att utöver grundförmågan verksamheten tillförs särskilda resurser för att förebygga och hantera händelser som kan leda till svåra påfrestningar på samhället. KBM identifierar tre delförmågor som bygger upp en sådan förstärkt förmåga, i fallande prioritetsordning:[114]

- Förmågan att leda, samordna och informera om hanteringen av krisförlopp som kan leda till svåra påfrestningar på samhället (krishanteringsförmåga).
- Förmågan att genomföra operativa insatser vid krisförlopp som kan leda till svåra påfrestningar på samhället (operativ förmåga).
- Förmågan hos den samhällsviktiga infrastrukturen att motstå störningar som kan leda till eller uppkomma vid svåra påfrestningar på samhället (förmågan hos samhällsviktiga infrastrukturen att motstå störningar).

Motivet för prioriteringen av krishanteringsförmågan är att inget skydd kan bli fullständigt och att samhället således alltid måste ha en förmåga att aktivt hantera en kris. Valet innebär emellertid att fokus för det svenska sektorsövergripande krisberedskapsarbetet snarare ligger på krishantering än på skydd av kritisk infrastruktur. Detta påverkar även resursflöden. Samtidigt kan såväl operativ förmåga som krishanteringsförmåga ha stor betydelse för förmågan att återställa kritisk infrastruktur.

I Sverige ägs samhällsviktig infrastruktur till stor del av privata aktörer. En utvecklad samverkan mellan offentlig sektor och näringsliv anses av regeringen utgöra en viktig del av den svenska strukturen för krishantering.[115] Det är sektorsmyndigheter (som t.ex. Post- och telestyrelsen, Statens Energimyndighet etc.) som ansvarar för denna samverkan.

Arbete med att utveckla privat-offentlig samverkan pågår och det finns exempel på fungerande samverkan inom flera områden. KBM arbetar med att ta fram en tydligare inriktning för sin verksamhet inom detta område. Ett förslag presenterades i rapporten ”Så vill vi utveckla krisberedskapen”[116]. Detta förslag innebar att

- samverkan mellan offentlig sektor och näringsliv bör etableras på nationell, regional och lokal nivå för att hantera krisberedskapsfrågor

[114] Krisberedskapsmyndigheten: *Samhällets krisberedskap. Inriktning av verksamheten 2007*, KBM Planeringsprocessen 2005:03, sidan 19.
[115] Regeringen: *Samhällets säkerhet och beredskap*, proposition 2001/02:158, 2002-03-14, sidan 50.
[116] Krisberedskapsmyndigheten: *Så vill vi utveckla krisberedskapen*, 2005, KBM:s dnr: 0418/2005.

- offentliga medel för samhällets säkerhet bör investeras i projekt som ger incitament för företagen att samverka
- säkerhets- och sårbarhetsfrågor bör beaktas i högre grad vid offentlig upphandling.

Post- och telestyrelsens (PTS) krisberedskapsverksamhet inom området elektroniska kommunikationer präglas av samverkan med privata tjänsteoperatörer och nätägare. En viktig del av PTS strategi är att i partnerskap samverka med de enskilda aktörerna inom elektronisk kommunikation med utnyttjande av ekonomiska incitament och överenskommelser till gemensam nytta.[117] Arbetet har tagit sig olika former, ett exempel är upphandling av mobila reservkraftsaggregat åt mobiltelefonoperatörer. Ett annat är de samfinansierade projekt som PTS utför tillsammans med Stadsnätsföreningen där man tar fram branschrekommendationer för ”Robusta nät”, ”Robusta noder”[118] och ”Nätdokumentation”[119] gällande för bredbandsnät.

Krisberedskapsmyndigheten har pekat på fyra olika huvudsakliga finansieringssätt för skyddsåtgärder som vidtas av privata aktörer. Frivilligt finansierade åtgärder, lagtvingad finansiering av åtgärder, finansiering genom avgift från sektorn eller finansiering via anslag. KBM pekar vidare på att avgiftsfinansiering har använts inom t.ex. telekomområdet med framgång men understryker att det troligen krävs en kombination av alla fyra finansieringsmetoderna.[120]

Vad avser finansieringen av fredstida förstärkt förmåga har regeringen i propositionen ”Vårt framtida försvar” gjort klart att dess övergripande ansvar för en fredstida förstärkt förmåga inte självklart skall översättas i ett finansieringsansvar utan att såväl näringsliv och organisationer som myndigheter har ett ansvar att skydda sin verksamhet från olika typer av störningar. Staten skall finansiera åtgärder för att bättre möta ”extrema situationer, motsvarande en svår påfrestning på samhället i fred, där det inte finns någon annan aktör som kan tillse att det finns en tillräcklig förmåga”. Detta exemplifieras med förberedelser för ledning, samordning, information och förmåga att agera under allvarlig kris. Utöver detta ”kan det behöva vissa förstärkningsresurser samt vissa tekniska förstärkningsåtgärder i den samhällsviktiga infrastrukturen”. Regeringen är också beredd att finansiera vissa åtgärder, såsom kunskapsuppbyggnad och

[117] Post- och telestyrelsen: *Robusta elektroniska kommunikationer – En strategi för åren 2003-2005*, PTS-ER-2003:13
[118] Svenska stadsnätsföreningen: *Robusta noder – Rekommendationer*, februari 2004
[119] Svenska stadsnätsföreningen: *Projektbeskrivning Nätdokumentation*, http://www.ssnf.org/data/312.pdf, 2004-03-11.
[120] Krisberedskapsmyndigheten: *Nya villkor för samhällets krisberedskap*, KBM:s uppdrag/utredningar 2004, sidan 82f.

övningsverksamhet för att stärka förmågan att ge hjälp till respektive ta emot hjälp från andra stater i en situation av allvarlig kris.[121]

Regeringen har i propositionen ”Vårt framtida försvar” hävdat att ett ökat internationellt engagemang bör ge ett mervärde för det svenska krishanteringssystemet genom erfarenhetsutbyte och samarbete. Utbildningsfrågor, kompetensutveckling och utveckling av interoperabilitet är några delar som understryks. Regeringen anser vidare att den planering och de förberedelser som genomförs inom EU-samarbetet för att underlätta medlemsstater att bistå varandra vid en kris ökar enskilda staters ”möjligheter att framgångsrikt hantera konsekvenser av mer omfattande kriser”.[122] Denna syn torde gälla även specifikt för skydd av kritisk infrastruktur.

Krisberedskapsmyndigheten har vidare noterat att eftersom kriser som uppstår i ett land kan fortplantas till ett annat är det viktigt att lära av varandra för att få ett så bra skydd som möjligt i så många stater som möjligt. Vidare menar KBM att internationellt samarbete kan underlätta för en stat att avropa andra staters resurser när de egna inte räcker till i krishanteringen.[123]

KBM understryker också nyttan av utbyte och samarbete kring forskning, erfarenhetshantering etc.[124] Mer specifikt menar Krisberedskapsmyndigheten att EU:s mervärde ligger i situationer där detta samarbete tillför kunskap och resurser som inte annars skulle kunna åstadkommas. Som exempel på detta nämner KBM identifiering av gemensamma sårbarheter, kunskapsuppbyggnad och erfarenhetsutbyte, underlättande av samverkan mellan näraliggande stater under en kris samt en roll som ”förmedlare” av resurser och information mellan stater.[125]

Regeringen anser att EU-samarbetet är centralt för svensk krishanteringsförmåga. Det svenska krisberedskapsarbetet kommer enligt regeringen bl.a. att påverkas av EU:s arbete med att förbättra Unionens och medlemsstaternas förmåga att bekämpa terrorism och skydda befolkningen mot allvarliga händelser. Regeringen menar att Sverige måste fortsätta att utveckla sitt engagemang på EU-området då detta är en av förutsättningarna för att stärka svensk krisberedskapsförmåga.[126] Även Krisberedskapsmyndigheten har understrukit vikten av

[121] Regeringen: *Vårt framtida försvar*, proposition 2004/05:5, 2004-09-23, sidorna 216f och 219.
[122] Regeringen: *Vårt framtida försvar*, proposition 2004/05:5, 2004-09-23, sidan 221.
[123] Krisberedskapsmyndigheten: *Svensk krisberedskap i internationellt samarbete*, KBM:s Uppdrag/utredningar 2005, sidan 17.
[124] Krisberedskapsmyndigheten: *Svensk krisberedskap i internationellt samarbete*, KBM:s Uppdrag/utredningar 2005, sidan 12f.
[125] Ibid, sidan 19f.
[126] Regeringen: *Vårt framtida försvar*, proposition 2004/05:5, 2004-09-23, sidan 221f.

den internationella dimensionen samt behovet av att aktivt påverka och utveckla EU-nivån.[127]

Sverige tycks således snarast se det huvudsakliga mervärdet i informations- och erfarenhetsutbyte än i gemensamma kriterier för urval av infrastrukturer och i gemensamma säkerhetsnivåer. Eftersom Sverige inte förhållit sig till frågan om vad som utgör ”europeisk kritisk infrastruktur” går det i nuläget inte att säga vilket mervärde Sverige ser för EU på denna nivå, t.ex. när det gäller infrastrukturer som sträcker sig över flera stater.

[127] Krisberedskapsmyndigheten: *Svensk krisberedskap i internationellt samarbete*, KBM:s Uppdrag/utredningar 2005, sidan 17.

5 Jämförande analys

5.1 Allmänt

I detta kapitel jämförs, utifrån de tidigare identifierade jämförelsefaktorerna, Sveriges politik för skydd av kritisk infrastruktur med den CIP-politik som nu diskuteras inom EU. När så är möjligt dras också några tentativa konsekvenser rörande identifierade skillnader och likheter. Dessa skall inte ses som uttömmande eller slutgiltiga utan snarast som hjälp och grund för vidare diskussion.

5.2 Vad utgör kritisk infrastruktur?

5.2.1 Vad utgör kritisk infrastruktur?

Det finns generellt sett en hög grad av samförstånd mellan europeiska stater när det gäller synen på vad som utgör kritisk infrastruktur och kritiska samhällstjänster. Det handlar i huvudsak om tekniska nätverk och centrala samhällsfunktioner (se bilaga 1 för en sammanställning av några staters och organisationers syn).

Såväl Sverige som Kommissionen tycks i huvudsak betrakta kritisk infrastruktur utifrån ett systemperspektiv, d.v.s. relativt nyttan för andra infrastrukturer eller för samhällstjänster. Skillnaden mellan det svenska systemet och det diskuterade EU-systemet för skydd av kritisk infrastruktur ligger istället i att medan Kommissionen vill se gemensamma kriterier och en harmoniserad analysgång för att identifiera kritisk infrastruktur, har Sverige hittills inte angett en tydlig definition av kritisk infrastruktur.

Den av Kommissionen i EPCIP-processen föreslagna EU-definitionen av kritisk infrastruktur innehåller referenser till vitala intressen (hälsa, säkerhet, ekonomi) vilka i sin tur kan ses som nödvändiga för att nå Unionens mål och upprätthålla Unionens grundläggande värden. I Sverige görs idag inte någon explicit koppling till värden, men i ett begrepp som ”samhällsviktig verksamhet” ligger implicit samhällsvärden. KBM:s regeringsuppdrag att definiera vad som avses med samhällsviktig verksamhet torde också beröra vad som är centrala samhällsvärden.[128] Om sedan i nästa steg de för de samhällsviktiga verksamheterna kritiska, stödjande infrastrukturerna identifieras så skapas även i Sverige en koppling mellan värden och kritisk infrastruktur. Vidare är skrivningarna om

[128] I en studie som FOI genomförde våren 2005 med avsikt att ta fram kriterier för att avgöra samhällsviktig verksamhet kunde också ur propositions- och försvarsberedningstexter identifieras ett antal tentativa, grundläggande värden och vitala samhällsintressen: Värna liv och hälsa, värna miljön, upprätthålla god samhällsekonomi och skydda ekonomiska värden, upprätthålla en demokratisk rättsstat och bevara fred och nationell självständighet. Birgitta Lewerentz et al: *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system*, FOI MEMO 1283, mars 2005, sidan 29ff.

Unionens värden och mål i fördragsutkastet, under förutsättning att det ratificeras, styrande för både EU:s och medlemsstaternas politikutformning.

EU-processen kommer att driva på utvecklingen av en svensk definition av kritisk infrastruktur. De kriterier för identifiering av kritisk infrastruktur som skulle ingå i en styrande EPCIP-process skulle behöva inkorporeras även i svensk, nationell analys och få konsekvenser för svensk prioritering av skyddsåtgärder. Då krävs att Sverige, för att kunna nå en påverkan i EU-processen, utvecklar en tydlig nationell bild av hur dessa kriterier bör se ut.

Även i en situation där EU:s roll snarast blir att stödja samordning och informationsutbyte mellan medlemsstaterna skulle svensk CIP-politik påverkas av den gradvisa ensning som skulle uppstå. Inte minst skulle konkurrensargument skapa ett tryck för likartat regelverk rörande vad som anses som kritisk infrastruktur.

5.2.2 Vad utgör transnationell kritisk infrastruktur?

Om EU får en konkret roll i skyddet av det som definieras som ”europeisk kritisk infrastruktur”, skild från den roll EU har relativt ”nationell kritisk infrastruktur”, kommer vad som definieras som sådan infrastruktur att bli en nyckelfråga. Ju vidare definitionen blir, desto större potentiellt inflytande kommer EU och Kommissionen att få över CIP-arbetet. Kommissionen har hittills också varit mer ivrig än Sverige att ange en definition. Sverige behöver därför nu, utifrån vilken roll man vill se för Kommissionen och EU, utveckla en mer exakt syn på kriterierna för att identifiera europeisk kritisk infrastruktur.

Kommissionens förslag till definition av europeisk infrastruktur har ett medlemsstatsperspektiv: den pekar ut sådan infrastruktur vars bortfall omedelbart eller över tiden skulle få allvarliga konsekvenser för vitala samhällsintressen, och i förlängningen grundläggande värden, i två eller flera medlemsstater. Däremot görs ingen koppling till europeiska värden. Å andra sidan tycks CIP i sakpolitikområden många gånger snarast syfta till upprätthållandet grundläggande EU-intressen som den inre marknaden och fri konkurrens. Försäkringsperspektivet – att inkludera sådan infrastruktur där hela EU är ett rimligt försäkringskollektiv – tycks däremot i stort osynligt i bägge fallen.

Sverige har hittills inte haft någon officiell syn på vad som bör utgöra transnationell eller ”europeisk” kritisk infrastruktur. Det tycks dock finnas ett pragmatiskt erkännande av att det existerar infrastruktur som i en mer konkret mening är transnationell därför behöver diskuteras på en internationell nivå. Samtidigt finns det en tveksamhet mot en definition av europeisk infrastruktur som innebär att EU får ett mer konkret, sektorsövergripande ansvar för skydd av kritisk infrastruktur.

Sverige har, tillsammans med flera andra medlemsstater, menat att en infrastruktur inte bör ses som transnationell/europeisk om den bara sträcker sig över två medlemsstater, utan att den i sådana fall borde behandlas som bilateral. Denna position innebär i så fall en ytterligare nivå bredvid nationell och europeisk och frågan blir om den skall hanteras som nationell infrastruktur av det gemensamma ramverket eller som något annat.

Det återstår vidare en rad avgränsningsfrågor vilka hittills inte berörts av vare sig EU eller Sverige. Innebär multinationalisering av ägare/operatörer att i grunden nationell infrastruktur som styrs från ett annat land skall ses som europeisk? Vad innebär tidskriteriet i Kommissionens förslag till definition för vad som skall räknas som europeisk infrastruktur? Det krävs en fördjupad diskussion kring frågor som dessa vid formulerandet av kriterier för identifiering av kritisk infrastruktur, oavsett vilken roll EU skall spela relativt sådan infrastruktur.

5.2.3 Hur identifieras kritisk infrastruktur och av vem?

EU och Sveriges förhållningssätt när det gäller hur kritisk infrastruktur definieras och identifieras ter sig tämligen väsenskilda. Kommissionen förespråkar ett EPCIP med en uppifrån och ned analysprocess, centraliserad med register över kritisk infrastruktur på nationell och europeisk nivå, och med utgångspunkt i vissa grundläggande samhällsintressen som värnandet av hälsa, säkerhet, fungerande stat. EPCIP skall utgöra ett gemensamt och harmoniserat analysramverk.

Denna centraliserade och styrda identifieringsprocess är främmande för det svenska systemet som hittills utgått från det vaga och icke-definierade begreppet samhällsviktig verksamhet och sedan i en nedifrån och upp förhandlingsprocess inom och mellan samverkansområden beslutat om fördelningen av medel för skydd av infrastruktur.[129] Redan idag är myndigheter och företag tidvis tveksamma till att lämna över allt för detaljerad information om kritiska infrastrukturer till nationella myndigheter som t.ex. KBM och det är inte svårt att se framför sig att denna tveksamhet kan komma att bli minst lika stor när det gäller att lämna över information till EU.

Utmaningen i att jämka samman det svenska systemet med ett EPCIP av det normerande slag som Kommissionen förespråkar blir särskilt tydlig när det

[129] Detta är naturligtvis en medveten generalisering – EU är i högsta grad ett organ för förhandlingar och det svenska systemet innehåller i högsta grad analys. Poängen är att i själva avgörandet av vad som utgör kritisk infrastruktur vill EU se en harmoniserad analys grundad på fastlagda kriterier medan Sverige har genomfört analyser hos myndigheter men värderingen mellan myndigheter och mellan samverkansområden skett i förhandlingar. Värden kan möjligen också, som konstaterades tidigare, vara på väg att bli en viktigare utgångspunkt även avseende svensk kritisk infrastruktur i och med processen att ta fram en definition av samhällsviktig verksamhet.

gäller hur ansvarsfördelningen skall se ut inom den svenska myndighetssfären. En fråga är vilken svensk myndighet som skall delta i arbetet med att utveckla den europeiska processen för identifiering av kritisk infrastruktur och dess kriterier. En annan fråga är vilken eller vilka myndigheter som skall ansvara för att i Sverige driva det konkreta identifieringsarbetet avseende nationell kritisk infrastruktur.

När det specifikt gäller *europeisk* kritisk infrastruktur föreslår Kommissionen att den tillsammans med medlemsstaterna skall driva identifieringsarbetet. Utfallet av denna process blir som tidigare konstaterats avgörande för vilket inflytande EU får över CIP-arbetet och därmed högst politiskt. Även här är därför en central fråga vilken myndighet eller myndigheter som från svensk sida skall delta i detta sektorsövergripande, europeiska analysarbete, men också här hur en sådan europeisk, analys passar in med den svenska ”nedifrån och upp” planeringsprocessen med självständiga myndigheter.

Ett sätt för Sverige att hantera skillnaderna mellan svensk och tänkt europeisk analysprocess skulle kunna vara att låta EU-processen ingå som ett försteg till det inriktningsdokument som KBM tar fram till den svenska planeringsprocessen. Den styrda, uppifrån och ned EPCIP-process som Kommissionen förespråkar kan emellertid resultera i att delvis andra infrastrukturer – såväl nationella som europeiska – pekas ut som kritiska än vad som skulle lyftas fram i nuvarande svensk process. Därmed påverkas också prioriteringen av resurser inom krisberedskapsarbetet och ”försteget” får stort inflytande över inriktningen av svenskt beredskapsarbete samtidigt som sakmyndigheternas roll blir marginaliserad.

Om EPCIP istället skulle fokusera på erfarenhetsutbyte, gemensamma analysmetoder och att stödja en ökad grad av koordination blir det lättare att inkorporera i det svenska systemet. Horisontella, sektorsövergripande arrangemang som utvecklas i en sådan modell skulle t.ex. kunna handla om utveckling av metoder och kriterier för att bedöma huruvida en infrastruktur är kritisk och en gradvis ensning av synen på vad som utgör kritisk infrastruktur på en europeisk nivå. Utvecklingen skulle kunna i stor utsträckning bygga på erfarenheterna från existerande CIP-samarbeten inom och utom EU-ram. Sakmyndigheterna skulle kunna delta i en sådan gradvis process och även lyfta in resultaten i sitt eget arbete. Emellertid skulle vägen till ett gemensam europeiskt synsätt rörande såväl horisontella som sektorsspecifika aspekter på CIP troligen bli längre.

I den svenska processen sker kontakterna med ägare och operatörer i huvudsak via sakansvariga samverkansmyndigheter. På så vis får denna kontakt en nedifrån och upp karaktär. Hur kontakterna i identifieringsprocessen skall se ut på EU-nivån är oklart men den typ av forum för åsiktsutbyte på en EU-nivå som

Kommissionen diskuterar skulle kunna vara en väg. Liknande metoder används redan inom flera sakområden, t.ex. den finansiella sektorn. Detta skulle emellertid kunna bli en process av mer uppifrån och ned karaktär där en bransch kommer överens om gemensamma ståndpunkter som de driver mot den ”högsta” nivån, EU, via sina branschrepresentanter.

5.3 Mot vad skall infrastrukturen skyddas?

5.3.1 Vad betraktas som relevanta hot?

Även om den nuvarande CIP-processen inom EU har sitt huvudsakliga ursprung i hotet från terrorismen finns det en bred acceptans bland medlemsstaterna för att hotbilden som beaktas bör vara ”all-hazards”, om än med ett särskilt fokus på terrorism. I sakområdena har dessutom CIP-arbetet hela tiden haft en hög grad av ”all-hazards”. Detta tycks således inte utgöra någon skiljefråga för svensk del.

När det gäller att skilja på mer normala störningar och extraordinära händelser kan konstateras att såväl EU som Sverige har ett intresse av att infrastrukturerna skall klara av att hantera bägge delar. Huruvida skydd mot störningar är något som EU-nivån blir involverad i torde dock variera från sektor till sektor. När det gäller infrastrukturer där även mindre ”störningar” kan leda till svåra konsekvenser (flygsäkerhet, kemanläggningar etc.) har EU redan idag en roll i att analysera händelser och lägga fast riktlinjer även vad gäller störningar. När det gäller andra områden, där en viss acceptans finns för störningar (elnät, informationsnät), har EU inte en sådan roll utan ansvaret har hittills helt legat hos medlemsstaterna. Samtidigt är det rimligt att tänka sig att känsligheten mot störningar måste tas med också i det sektorsövergripande EU-arbetet, inte minst på grund av de beroenden som kan finnas mellan infrastrukturer.

För Sverige innebär ansvarsprincipen att hela spektrumet från störningar till extraordinära händelser i möjligaste mån skall hanteras av samma organisationer och med samma resurser. Det betyder att även om EU inte ges en roll avseende mindre störningar så kommer CIP-åtgärder för att hantera extraordinära händelser också att påverka svensk organisation och svenska åtgärder för att hantera störningar.

5.3.2 Hur definieras hotet och av vem?

EU:s medlemsstater uttryckte i solidaritetsprogrammet att medlemsstaterna i sitt nationella arbete bör bättre utnyttja de hotanalyser som Rådssekretariatets lägescentral (Situation Centre) och EUROPOL arbetar fram. För den svenska planeringsprocessen skulle detta generellt sett inte behöva innebära någon större komplikation utan kunna utgöra ytterligare ett underlag i den hotbild som fungerar som en utgångspunkt i arbetet. Sverige deltar redan idag aktivt såväl i läges-

centralens som EUROPOLs underrättelsesamarbete, både i formulerandet av underrättelsebehov och i det praktiska arbetet, och detta skulle kunna utvidgas även till CIP-relaterade hot.

En gemensam hotuppfattning kan utgöra en god bas också för samarbete rörande skydd av kritisk infrastruktur. Emellertid sätter en gemensam, normerande hot-uppfattning på både gott och ont agendan och styr i en förlängning också var resurserna för skydd – oavsett om de är förebyggande, förberedande eller återställande – behöver sättas in. Det innebär också att det finns risk för en överdriven likriktning över EU: ett hot mot svensk infrastruktur behöver inte vara ett hot mot grekisk infrastruktur. Här finns också möjligen en skillnad relativt underrättelseanalyserna inom ramen för utrikes- och säkerhetspolitiken som i de allra flesta fall endast ligger till grund för gemensamma uttalanden eller andra diplomatiska ageranden där medlemsstaterna ofta har ett gemensamt intresse. Sverige behöver en strategi för hur man skall förhålla sig till detta och i vilken grad Sverige anser att eventuella ”normerande” underrättelsebedömningar, som skulle kunna komma påverka nationella riskanalyser och resursprioriteringar, skall få förekomma i EPCIP-ramverket.

Kommissionen vill slutligen se CIWIN (Critical Infrastructure Warning and Information Network) som ett nätverk även för kortsiktiga underrättelser och snabb varning. Det finns emellertid redan ett antal varningsnätverk i olika sektorer och det har framförts att det är tveksamt om ett sektorsövergripande varningsnätverk verkligen skulle tillföra något. Om CIWIN ändå skulle få en underrättelseroll så uppstår för svensk del en fråga om ett sådant ”snabbt” varningssystem kan gå via en sektorsövergripande, nationell EPCIP-myndighet som med stor sannolikhet inte kommer att vara en underrättelsemyndighet och dessutom troligen, som det svenska systemet ser ut idag, inte kommer att ha direkt kontakt med ägare/operatörer i olika infrastruktursektorer.

5.4 Hur skall skyddet utformas?

5.4.1 Vilken fas av skyddsarbetet lägger man tonvikten på?

I de diskussioner som nu förs ligger EU:s tonvikt avseende CIP på förebyggande och förberedande åtgärder. Den enskilda medlemsstaten, inklusive Sverige, måste däremot arbeta med skyddets alla faser. Detta utgör en principiell skillnad i utgångspunkt för arbetet med CIP i EU respektive Sverige. För EU är CIP ett område som i stort tycks stå för sig själv även om det finns en koppling till kampen mot terrorism och även om CIP i enskilda politikområden har motiverats med stöd till europeiska intressen. CIP ingår däremot inte, som är fallet

för medlemsstaterna, i en större intern krisberedskapskontext av det enkla skälet att EU inte, åtminstone inte ännu, har någon sådan.[130]

För Sverige utgör skydd av kritisk infrastruktur en del av krisberedskapsarbetet i stort, och prioritering av resurser görs inte bara mellan olika infrastrukturer och mellan olika faser utan även mellan skydd av kritisk infrastruktur och andra krisberedskapsinsatser. En sådan tydlig prioritering i det svenska systemet är att krishanteringsförmåga (att kunna leda, samordna och informera om hanteringen av krisförlopp) ses som högre prioriterat än skyddet av kritisk infrastruktur. Här kan uppstå en konflikt mellan svenska och europeiska prioriteringar avseende skydd av kritisk infrastruktur. Denna konflikt blir tydligast i ett styrande och normerande EPCIP av det slag Kommissionen diskuterat men kan även uppstå i ett EPCIP som mer handlar om att stödja informations- och erfarenhetsutbyte och gemensam metodutveckling. Om ett stort antal medlemsstater har en annan syn än Sverige på hur prioriteringen skall se ut blir det i bägge fallen i längden svårt att hålla fast vid ett specifikt svenskt synsätt.

När det gäller av EU samordnade resurser för mer konkreta insatser t.ex. för återställande av infrastruktur handlar detta troligen snarast om insatser vid större katastrofer och ligger på gränsen till det som kan kallas konsekvenshantering. Det svenska systemet behöver analysera i vilka typer av situationer sådant stöd skulle kunna bli aktuellt och hur det då skulle se ut. Därefter kan Sverige utveckla förmågan att ge och ta sådant stöd liksom nödvändigt regelverk.

Regeringen har i propositionen ”Vårt framtida försvar” förklarat sig beredd att satsa pengar på ett utvecklingsarbete rörande dessa frågor. Här skulle kunna finnas ett slags försäkringsmervärde för Sverige men det krävs då troligen att Sverige tidigt är med och påverkar vilka resurser och i vilka situationer sådant stöd kan bli aktuellt. Olika stater kommer med stor sannolikhet att vilja prioritera olika behov och problem. Programmet för säkerhet och skydd av friheter innehåller sedan möjligheter att finansiera olika projekt för att utveckla förmåga och planering samtidigt som det t.ex. inom räddningstjänstområdet redan sker en utveckling av t.ex. interopearabilitet.

5.4.2 Vilken karaktär skall multinationella åtgärder för skydd av kritisk infrastruktur få?

Kommissionen förespråkar ett EPCIP som utgör ett sektorsövergripande ramverk innehållande gemensamma miniminormer för säkerhet hos kritiska infrastrukturer och uppföljande inspektioner. Kommissionen vill också att delar av eller hela detta ramverk skall infogas i ett för nationell lagstiftning styrande

[130] Här skall dock sägas att bl.a. Haagprogrammet och utvecklingen av de ”integrerade krishanteringsarrangemang”, tillsammans med ARGUS och Kommissionens eget krishanteringssystem (se avsnitt 3.1), kan ses som ett försök att skapa en sådan kontext.

ramdirektiv. Mot detta står en bild, framförallt i av Rådet beslutade program och strategier, av ett EPCIP som mer handlar om att stödja framväxten av en ökad grad av koordination och samverkan mellan medlemsstaterna avseende CIP.

Tittar man på existerande EU-samarbete i sakpolitikområden finns där en blandning av modeller som går från gemensamma styrande säkerhetsregler, uppföljda av Kommissionen via övergripande målsättningar som sätts upp gemensamt men som fylls av regler och säkerhetsnivåer nationellt till icke-bindande rekommendationer.

Sverige menar att mervärdet i det multilaterala arbetet med CIP snarast ligger i erfarenhets- och informationsutbyte, ”best practices” etc. Därmed ligger Sverige närmare den roll för EU som handlar om att stödja samordning och informationsutbyte.

Samtidigt har Krisberedskapsmyndigheten menat att det svenska systemet för grundläggande säkerhetskrav på samhällsviktig verksamhet är heterogent, med stora skillnader i analys och resultat mellan områden. Detta kan, enligt Krisberedskapsmyndigheten, skapa problem t.ex. när områden som är beroende av varandra har olika syn på säkerhetsnivåer. KBM har därför argumenterat för en översyn av vilka krav som bör ställas på samhällsviktig verksamhet.[131]

Med en sådan utveckling skulle det svenska systemet närma sig det EPCIP som Kommissionen diskuterar. En utveckling av miniminormer på EU-nivån, såväl på ett principiellt plan (hur de i principiell mening konstrueras och uttrycks) som i konkreta termer (vilka de rent konkret är), skulle därför vara ett centralt område för Sverige att följa och påverka. Om ett sådant system skulle införas skulle dess normer sannolikt i hög utsträckning bli styrande även för svenska grundläggande säkerhetskrav.

Här kan också finnas en skillnad mellan det som definieras som europeisk och det definieras som nationell kritisk infrastruktur. Om en infrastruktur ses som kritisk på europeisk nivå, t.ex. på grund av beroenden mellan infrastrukturer i olika medlemsstater, kan det vara lättare att acceptera behovet av prioritering och säkerhetsnivåer som läggs fast, och eventuellt även följs upp, av EU. Det kan samtidigt vara värt att notera att samma argument som KBM använder för utveckling av grundläggande säkerhetsnormer i Sverige går att använda för en fördjupad sektorsövergripande EU-styrd analys av såväl nationell som europeisk kritisk infrastruktur.

[131] Krisberedskapsmyndigheten: *Nya villkor för samhällets krisberedskap*, KBM:s uppdrag/utredningar 2004, sidan 74ff.

5.4.3 Vem ansvarar för skyddet av kritisk infrastruktur?

I grunden skulle ett EPCIP som Kommissionen beskriver det utgöra ett sektorsövergripande, centraliserat system, som samlar information om såväl infrastrukturer som vidtagna skyddsåtgärder på två olika nivåer, den nationella och den europeiska. En centralt fastlagd identifierings-, analys- och prioriteringsprocess skulle styra arbetet. Detta till skillnad från det svenska systemet som är decentraliserat utan några centrala register och utan någon stark, styrande analysprocess för att identifiera och prioritera CIP-insatser.

Hur vittomfattande EU:s roll skulle bli, avgörs delvis av hur kriterierna för att identifiera europeisk respektive nationell kritisk infrastruktur formuleras. Unionens roll är i Kommissionens grönpapper betydligt större för europeisk kritisk infrastruktur. Samtidigt förespråkar Kommissionen att EPCIP även bör utgöra ett ramverk för medlemsstaternas arbete med nationell kritisk infrastruktur.

Ett EPCIP som det som Kommissionen förespråkat skulle därför få konsekvenser för Sverige. För det första på ett principiellt plan – var skall beslut rörande CIP tas och i vilken mån kan Sverige bibehålla ett nedifrån och upp system. För det andra mer konkret, organistoriskt – vilken myndighet skall pekas ut som svensk ”EPCIP-myndighet” och hur skall denna förhålla sig till de sakansvariga myndigheterna.

Sakområdesdirektiv från EU skulle även med EPCIP kunna fortsätta att gå till myndigheter med sakansvar. Sakmyndigheter skulle också kunna delta i sektorsspecifika diskussioner på EU-nivån, även om formatet för sådana diskussioner återstår att utveckla. Däremot är en utestående fråga hur sektorsövergripand, horisontella CIP-direktiv skall hanteras på svensk nivå. Blir EU:s inriktningar faktorer som skickas vidare till samverkansmyndigheterna i inriktningsdokumenten för planeringsprocessen och skall då Krisberedskapsmyndigheten utveckla sin samordnande roll eller finns det andra lösningar t.ex. att även detta är något som sakmyndigheter får med sig från eget deltagande i EU-processer?

Detta väcker också frågan om vilken eller vilka svenska myndigheter som skulle representera Sverige i EU när sektorsövergripande CIP-frågor skall diskuteras. Naturligt är att utpekad EPCIP-myndighet får en central roll men en sådan myndighet sitter knappast på all relevant sakkunskap. På ett sakpolitikområde där flera myndigheter är involverade, informationssäkerhetsområdet, har Sverige löst frågan genom att åsätta UD som svensk kontaktpunkt och svensk säkerhetsmyndighet. En liknande lösning skulle vara möjlig för sektorsövergripande CIP-frågor men innebär samtidigt att svensk representant i EU-samarbetet hamnar långt från sakfrågearbetet.

Liknande frågor måste emellertid också ställas inom EU och Kommissionen. Vilken del av EU skall horisontellt koordinera sakpolitikområdenas direktorat när det gäller CIP och hur ser direktoraten på detta? Var skall det praktiska CIP-arbetet, att förbereda beslut, utarbeta kriterier och genomföra inspektioner ligga? Även andra medlemsstater har liknande frågor att ta ställning till.

När det gäller relationen till privata aktörer och ägare av infrastruktur understryks i Kommissionens förslag att ett aktivt partnerskap bör upprättas på såväl nationell som internationell nivå. Bland annat vill Kommissionen skapa ”forum för åsiktsutbyte” och stödja framväxt av branschorganisationer rörande CIP. Mer exakt hur detta partnerskap skall se ut och dess närmare roll och uppgifter berörs dock inte. Inte heller berörs fördelningen av ansvar för samverkan mellan den internationella och nationella nivån. För transnationella infrastrukturer med olika ägare/operatörer i olika medlemsstater kan samverkan på en EU-nivå emellertid utgöra ett mervärde.

I Sverige pågår för närvarande en diskussion när det gäller hur relationen mellan samhället och ägare/operatörer skall se ut. Centrala frågor är i vilken utsträckning överenskommelser skall vara frivilliga eller lagstyrda, och bl.a. KBM har menat att en kombination av olika instrument kan vara nödvändig. EPCIPs natur av centralt styrt program med miniminormer för säkerheten skulle kunna innebära ett mer lagstyrt förhållningssätt till ägare/operatörer.[132] Här kan finnas skillnader i synsätt mellan olika medlemsstater men också mellan medlemsstater och EU.

Troligt är att EU:s påverkan på det svenska arbetet med CIP måste tas med såväl i planering inom specifika sektorer som i krisberedskapssystemets och samverkansområdenas planeringsprocesser. Det krävs därför en sektorsövergripande samordning, men också ett stöd till enskilda myndigheter och samverkansområden när det gäller EU-frågor. Detta är en slutsats som berörts även i tidigare studier av EU:s framväxande system för intern krishantering.[133]

5.4.4 Hur finansieras skydd av kritisk infrastruktur?

Kommissionen, liksom Sverige, menar att huvuddelen av finansieringsansvaret för att skydda anläggningar ligger hos operatörer och ägare. I den modell för EPCIP som Kommissionen lyft fram innebär utpekandet av infrastruktur potentiellt omfattande kostnader, framförallt när det gäller åtgärder för ökat skydd. EU kan bidra med medel till forskning och för upprättande av olika former av gränsöverskridande arrangemang. Inom vissa sakpolitikområden diskuteras också

[132] Dock kan även ägare/operatörer i vissa lägen vilja se i lag fastställda regelverk, inte minst för att tillse ett konkurrensneutralt säkerhetsarbete. En central fråga blir emellertid vem som skall stå för notan för att implementera ett sådant regelverk.
[133] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, sidan 78ff.

möjligheten till projekt definierade av EU för att höja säkerheten hos enskilda infrastrukturer. Sådan gemensam finansiering av skyddsåtgärder ter sig emellertid som undantag.

För skyddsinsatser som utgör del av ett större samhällsintresse anser dock Kommissionen att samhället måste ta ett större finansieringsansvar. Ägare/-operatörer kan inte förväntas bära hela denna börda själv. I Sverige har i praktiken mycket av åtgärderna finansierats antingen via avgifter eller via lagtvingande säkerhetsåtgärder. KBM har noterat att det kan vara svårt att dra gränsen mellan grund- och tilläggssäkerhet. Den diskussionen har ännu inte förts på EU-nivån och det ter sig troligt att olika medlemsstater har olika syn på hur gränsen skall dras vilket skulle försvåra finansieringsdiskussionerna.

Vidare kan olika medlemsstater ha olika syn på finansieringsformer. Är t.ex. avgiftsfinansiering självklart i hela EU för telekommunikationsområdet? EU:s medlemsstater har dessutom nått olika långt i avreglering av de tunga tekniska infrastrukturerna vilket också kan påverka synen på finansieringsformerna för CIP. En harmonisering av synen på finansieringsformer för CIP inom olika sektorer kan här vara nödvändigt, inte minst av konkurrensskäl. Konsekvenserna av en sådan ensning kan emellertid behöva utredas vidare sektorsvis – det är inte säkert att en sådan harmonisering alltid skulle sammanfalla med Sveriges nuvarande politik.

6 Avslutande diskussion

En avgränsning för denna rapport var att fokus ligger på EU:s initiativ och processer rörande skydd av kritisk infrastruktur. Det noterades emellertid redan i inledningen att synen på CIP hos medlemsstaterna, särskilt de stora, kommer att ha ett stort inflytande på det slutliga utformandet av en europeisk politik för CIP. Rapportens fokus innebär att detta inflytande riskerar att underskattas. Detta avslutande kapitel återkopplar därför delvis till medlemsstatsdimensionen.

Det har varit långt ifrån självklart att EU skall få en omfattande roll avseende skyddet av kritisk infrastruktur, CIP. De flesta medlemsstater har tvärtom ansett att skyddet av infrastruktur är, och bör vara, en i huvudsak nationell kompetens samtidigt som de ställt sig frågande till vilket mervärde EU kan tillföra. Det innebär dock inte att de inte kan se infrastruktur som ett övernationellt intresse, t.ex. beroende på att strukturer i olika stater är knutna till varandra.

De senaste årens utveckling av hotbilden, tillsammans med en ökad medvetenhet om infrastruktursystemens interdependens, har samtidigt inte bara inneburit att frågeställningen blivit mer aktuell utan också mer komplex. Det går inte längre att enkelt att avfärda diskussionen med att en viss institution har eller inte har formell befogenhet rörande ett visst område – om ett avbrott kan få effekter på en europeisk nivå är det också en potentiell EU-fråga. Det skall inte heller uteslutas att CIP är ett område där medborgarna faktiskt förväntar sig samarbete på EU-nivån.[134]

De två huvudsakliga roller för EU avseende CIP som framtonar ur EU-dokumenten – en centraliserande och styrande roll respektive en koordinerande och stödjande – ställs ibland i diskussionerna mot varandra. De är emellertid inte ömsesidigt uteslutande och bägge kan vara nödvändiga. Även med en i huvudsak styrande, uppifrån och ned-process krävs arrangemang för utveckling av kunskap och utbyte av erfarenheter och best practice.

Det är frestande att betrakta ett EPCIP vars huvuduppgift är att underlätta samordning som en parallell till den roll Krisberedskapsmyndigheten har visavi svenska myndigheter. I bägge fall handlar det om att samordna utan att styra, att lägga förslag om övergripande prioriteringar utan att ta över myndigheternas – i EU:s fall staternas – ansvar vare sig för beredskapsarbete eller operativ hantering. Det som KBM har men EU inte skulle få i denna roll är ett tydligt ansvar för att driva en planeringsprocess vilken bl.a. fördelar medel för skyddsåtgärder.

[134] I den två gånger per år publicerade Eurobarometern hamnar säkerhetsfrågor (fred och säkerhet i Europa, kamp mot organiserad brottslighet och kamp mot terrorism) regelmässigt högt upp i listan över av medborgarna prioriterade områden för EU.

I ett EPCIP som hamnar närmare det Kommissionen förespråkat får EU däremot ett tydligt ansvar för en europeisk planeringsprocess. Liksom är fallet för Sverige och KBM utgör detta en sektorsövergripande funktion med potentiellt stort ansvar för samordning och processledning av CIP men utan någon operativ roll. Skillnaden mellan KBM och EU blir emellertid att Kommissionen vill se en centraliserad, uppifrån och ned-process för EPCIP vilken inte på ett enkelt sätt skulle gå att samordna med det svenska systemets förhandlingstunga, nedifrån och upp-process.

Att det blir ett europeiskt program för skydd av kritisk infrastruktur som innebär någon form av koordination, sammanlänkning och utveckling av medlemsstaternas CIP-arbete är beslutat, men det är ännu oklart hur detta slutligen kommer att utformas. Även om hotet från terrorismen är en pådrivande faktor finns det hos många medlemsstater fortfarande en stor tveksamhet inför att lämna över sektorsövergripande befogenheter avseende CIP till EU då detta skulle innebära, direkt eller indirekt, EU-inflytande över medlemsstaternas nationella arbete med CIP. Det stöd som processen hade i utkastet till nytt fördrag – där skydd och beredskap är inskrivet som ett område där EU skall ha en kompletterande och stödjande roll – har dessutom i och med stoppet i ratificeringsprocessen kommit att försvagas.

Det återstår också flera frågor att lösa innan ett EPCIP kan fungera. Det handlar t.ex. på EU-nivån om organisatoriska frågor som var det sektorsövergripande CIP-arbetet skall bedrivas och hur detta skall kopplas till det som görs inom sakområden. Det handlar på EU-nivån också mer konkret om vilken infrastruktur som skall räknas som kritisk och vilken roll EU skall ha i utvecklingen av skyddet och i kontakter med operatörer och ägare.

Utmaningarna för Sverige speglar många gånger frågorna på EU-nivån:

- Skall Sverige överhuvudtaget acceptera att EU får en för medlemsstaterna styrande, sektorsövergripande roll?
- Vad är riskerna med att inte ha det?
- Vilket mervärde för EU ser Sverige på CIP-området generellt och inom vilka infrastruktursektorer anser Sverige att en ökad EU-roll är positiv?
- Hur skall denna EU-roll i så fall se ut?
- Hur skulle svenska konkreta prioriteringar rörande krisberedskap påverkas av en eventuellt EU-ledd identifierings- och analysprocess?
- Hur skall det svenska nedifrån och upp systemet med självständiga myndigheter hantera en sådan EU-roll?

- Vilka myndigheter skall få huvudansvar i den svenska processen och hur skall detta ansvar se ut?

Det skall understrykas att de former för EPCIP som Kommissionen drivit inte heller är de enda tänkbara. Istället för ett styrande, centralistiskt EPCIP byggt på ett ramdirektiv är det möjligt att istället se framför sig ett EPCIP som bygger på några politiskt överenskomna grundprinciper för CIP och samarbete kring CIP-relaterade frågor inom ramen för vilka medlemsstaterna förbinder sig att öka graden av samsyn och harmonisering. Till detta skulle kunna läggas en tämligen omfattande, och för harmoniseringsprocessen stödjande roll, i att utveckla den kunskap om hot, risker, sårbarheter och skyddsåtgärder (och metoder för att analysera dessa) som unionens medlemsstater bygger sitt arbete på. Det vore ett EPCIP närmare den ”mjukare” variant framtonat i t.ex. Haag- och Solidaritets-programmen.

EPCIP är således sammantaget fortfarande vagt i konturerna. Därmed finns det ett utrymme för ett proaktivt svenskt agerande för att påverka den slutliga utformningen av EU:s arbete med skydd av kritisk infrastruktur. I ett sådant agerande ingår såväl att lägga offensiva förslag som att bygga allianser med andra likasinnade medlemsstater. Det kräver emellertid att Sverige skaffar sig en tydlig bild av vad man anser vara nödvändigt och önskvärt att uppnå med ett EPCIP och vilket pris i form av EU-inflytande över CIP som är rimligt att betala för detta. Utifrån svaren på dessa frågor kan sedan en svensk linje formuleras avseende konkreta sakfrågor som kriterier för att identifiera kritisk infrastruktur, hur processen för att identifiera och analysera infrastruktur skall se ut, finansieringsformer etc.

7 Bilagor

Bilaga 1. Kritisk infrastruktur - några staters och organisationers definitioner och avgränsningar[135]

Här presenteras i punktform ett antal staters samt Natos och EU:s definitioner och avgränsningar gällande kritisk infrastruktur. Staterna är valda utifrån tre kriterier: Sådana som är politiskt ”ledande” i en europeisk kontext (Frankrike, Tyskland och Storbritannien), sådana som är ”lika” Sverige, framförallt storleksmässigt i en europeisk kontext (Finland, Norge, Nederländerna) samt slutligen några representanter för sådana utomeuropeiska stater som är ledande inom området skydd av kritisk infrastruktur (USA, Kanada).

Finland

I Finland definieras kritisk infrastruktur som följande sektorer:

- Bank- och finansväsende,
- Energiförsörjning,
- Livsmedelsförsörjning,
- Informations- och kommunikationsteknologisektorn,
- Försvarsrelaterad industri,
- Media,
- Folkhälsa,
- Samhällstjänster,
- Räddningstjänster,
- Social välfärd,
- Transport och logistik,
- Vattenförsörjning.

Frankrike

I Frankrike definieras kritisk infrastruktur som följande sektorer:

- Bank- och finansväsende,
- Kemisk och bioteknisk industri,
- Energi och elektricitet,
- Kärnkraftverk,
- Folkhälsa,
- Säkerhet och ordning,

[135] Informationen nedan om enskilda staters områdesindelning för kritisk infrastruktur är, när inget annat sägs, hämtad från Andreas Wenger, Jan Metzger: *International CIIP Handbook 2004*, Centre for Security Studies, Zürich 2004. Eftersom dessa indelningar bara skall användas som kontext och bakgrund för den europeiska och svenska utvecklingen har endast en begränsad uppföljning av informationens aktualitet och korrekthet genomförts. Förändringar kan således ha skett.

- Telekommunikationer,
- Transportsystem,
- Vattenförsörjning.

Nederländerna

I Nederländerna definieras kritisk infrastruktur som följande sektorer:

- Dricksvatten,
- Energi,
- Finansväsende,
- Livsmedel,
- Hälsa/hälsovård,
- Rättsväsende,
- Allmän ordning och säkerhet,
- Kontroll av kvalitet och kvantitet hos ytvatten,
- Telekommunikationer (inklusive Internettillgång, post etc.),
- Statsmakten,
- Transporter.

Norge

I Norge definieras kritisk infrastruktur som följande sektorer:

- Bank- och finansväsende,
- Statsmakt/administration,
- (Tele-) kommunikationer,
- Försvar,
- Energi,
- Olje- och gasförsörjning,
- Polis,
- Folkhälsa,
- Räddningstjänster,
- Social säkerhet,
- Transporter,
- Vattenförsörjning och avlopp.

Storbritannien[136]

I Storbritannien definieras kritisk infrastruktur som följande sektorer:

- Kommunikationer (ej transporter),
- Blåljusfunktioner,

[136] Se även http://www.niscc.gov.uk/niscc/aboutCNI-en.html.

- Energi,
- Finansväsende,
- Livsmedel,
- Regering och statsmakt,
- Risker och allmän säkerhet,
- Hälsa (hälsovård och folkhälsa),
- Transporter,
- Vatten och avlopp.

Tyskland

I Tyskland definieras kritisk infrastruktur som följande sektorer:

- Bank-, finans- och försäkringsväsende,
- Blåljusfunktioner,
- Energiförsörjning,
- Regering och statsmakt,
- Hälsa (inkl. vatten- och livsmedelsförsörjning),
- Telekommunikationer,
- Transporter.

Kanada

I Kanada definieras kritisk infrastruktur som följande sektorer:

- Kommunikations- och informationsteknologi
- Energi,
- Finansväsende,
- Livsmedel,
- Statsmakt,
- Hälsovård,
- Viss tillverkning (kemi, försvar etc),
- Säkerhet (CBRN, farliga ämnen och blåljusfunktioner),
- Transporter,
- Vattenförsörjning (inklusive avlopp).

USA

I USA definieras kritisk infrastruktur som följande sektorer:

- Jordbruk och livsmedel,
- Bank- och finansväsende,
- Kemikalier och farliga ämnen,
- Försvarsindustri,
- Räddningstjänster,

- Energi,
- Högre utbildning,
- Försäkringsväsende,
- Rättsväsende,
- Olja och gas,
- Post och distributionssystem,
- Folkhälsa,
- Telekommunikation och informationsteknik,
- Transporter,
- Vatten.

Utöver dessa identifieras kommersiella nyckeltillgångar, dammar, regeringsbyggnader, nationella monument och symboler samt kärnkraftsverk som viktiga att skydda.

Nato[137]

Natos definition av kritisk infrastruktur lyder:

> Critical infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government.

De sektorer som pekas ut är:

- Livsmedel,
- Energi,
- Nationella monument och symboler,
- Kemisk industri,
- Transporter,
- Jordbruk,
- Bank- och finansväsende,
- Post- och distributionssektorn,
- Försvarsindustrin,
- Hälsovård och räddningstjänster,
- Informations- och telekommunikationssystem,
- Vatten.

[137] NATO/EAPC: *Critical Infrastructure Protection – Concept Paper*, EAPC(SCEPC)D(2003)15, 2003-11-10.

Natos politik för skydd av kritisk infrastruktur är emellertid nära kopplat till alliansens arbete med Civil Emergency Planning (CEP). Som det uttrycks av Nato: ”aktiviteter syftande till att skydda kritisk infrastruktur bidrar också till förmågan att hantera effekten av katastrofer på befolkning och egendom”.[138]

Kritisk infrastruktur enligt EU

Det har visat sig svårt att komma överens på en europeisk nivå om vad som är kritisk infrastruktur. Kommissionen har i ett meddelande föreslagit att följande tentativa lista över kritiska infrastrukturer:[139]

- Energiinstallationer och nätverk,
- Kommunikations- och informationsteknik,
- Finanssystem,
- Hälsovård,
- Livsmedel,
- Vatten,
- Transporter,
- Produktion, lagring och transport av farligt gods (CBRN),
- Statsmakten (i vid mening).

Detta Kommissionsförslag till indelning utgör en tämligen konkret lista.

Under EPCIP-processen har Kommissionen också presenterat en mer utvecklad, indikativ lista över sektorer med kritisk infrastruktur:[140]

Sector	**Product or service**
I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines 2 Electricity generation 3 Transmission of electricity, gas and oil 4 Distribution of electricity, gas and oil
II Information, Communication Technologies, ICT	5 Information system and network protection 6 Instrumentation automation and control systems (SCADA etc.) 7 Internet8 Provision of fixed telecommunications

[138] Ibid.
[139] Commission of the European Union: *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702, 2004-10-20. Detta papper är inte ett officiellt kommissionsdokument och redovisar därmed inte nödvändigtvis Kommissionens samlade syn.
[140] Commission of the European Union: *Green paper on a European Programme for critical infrastructure protection*, COM(2005)576, 2005-11-17, sidan 24.

	9 Provision of mobile telecommunications 10 Radio communication and navigation 11 Satellite communication 12 Broadcasting
III Water	13 Provision of drinking water 14 Control of water quality 15 Stemming and control of water quantity
IV Food	16 Provision of food and safeguarding food safety and security
V Health	17 Medical and hospital care 18 Medicines, serums, vaccines and pharmaceuticals 19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/payment structures (private)
VII Public & Legal Order and Safety	21 Government financial assignment 22 Maintaining public & legal order, safety and security
VIII Civil administration	23 Administration of justice and detention 24 Government functions 25 Armed forces 26 Civil administration services 27 Emergency services 28 Postal and courier services
IX Transport	29 Road transport 30 Rail transport 31 Air traffic 32 Inland waterways transport 33 Ocean and short-sea shipping
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances 35 Pipelines of dangerous goods (chemical substances)
XI Space and Research	36 Space 37 Research

Bilaga 2. Skydd av kritisk infrastruktur i enskilda politikområden

EU har haft ansvar för åtgärder rörande CIP i ett antal specifika sakpolitikområden. För att få en uppfattning om hur EU arbetar med CIP är det därför centralt att titta på några sådana exempel. Följande områden har valts ut att studera närmare:

Eldistributionsnät samt informations- och kommunikationsnät för att dessa områden är centrala delar av det som ibland kallas för teknisk infrastruktur. Skydd mot farliga ämnen eftersom SEVESO II direktivet ofta lyfts fram som ett exempel på EU:s CIP-relaterade arbete. Flyg- och sjösäkerhet för att dessa är i fokus för kampen mot terrorismen och har genomgått en omfattande utveckling de senaste åren. Vattenhantering och livsmedelssektorn för att dessa är centrala för människors överlevnad och slutligen bank och finanssektorn eftersom denna är grundbulten för en fungerande samhällsekonomi.

Det är i denna rapport inte möjligt att göra fullständiga och djupa genomgångar av varje enskilt område utan fokus ligger på att beskriva EU:s roll i arbetet.

Eldistributionsnät

EU har diskuterat olika aspekter av energiförsörjningssäkerhet sedan åtminstone slutet av sextiotalet då det lagstiftades om miniminivåer för lager av olja och andra petroliumprodukter.[141] Kommissionen gav år 2000 ut ett grönpapper på temat energiförsörjningssäkerhet.[142]

När det gäller distributionen av energi (elektricitet men också olja och gas) stödjer EU utvecklingen av de så kallade Transeuropeiska Energinäten (TEN-E). Syftet är att bygga trans-nationella nät för att reducera energipriset, stödja fattigare delar av Unionen samt att säkra energitillgången. TEN-E fokuserar däremot inte på att finansiera åtgärder för att öka systemens robusthet eller för att skydda energiinfrastruktur mot specifika hot utan det är kraven som följer av utvecklingen av den inre marknadens som har styrt valet av projekt.[143] Emellertid kan hela projektet ses som att skapa en mängd fungerande distributionslinjer och minska beroendet av en eller ett fåtal linjer.

[141] Se europa.eu.int/scadplus/leg/en/lvb/127045.htm.
[142] Commission of the European Union: *Towards a European strategy for security of energy supply*, COM(2000)769.
[143] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, FOI juni 2005, sidan 23f. European Union: *Decision No 1229/2003/EC of the European Parliament an of the Council of 26 June 2003 laying down a series of guidelines for trans-European energy networks and repealing Decision No 1254/96/EC*.

Hittills har det inte funnits någon europeisk lagstiftning för skydd av eldistributionssystem mot olyckor utan existerande lagstiftning fokuserar istället på tillräcklig kapacitet inom medlemsstaterna. Medlemsstaterna definierar själva säkerhetskraven.[144]

EU:s institutioner behandlar i skrivande stund ett förslag till direktiv rörande tryggandet av elförsörjning och infrastrukturinvesteringar.[145] I detta ges medlemsstaterna ansvar för att utarbeta strategier för att trygga elförsörjningen. Medlemsstaterna skall bl.a. tillse att ”systemansvariga” uppfyller ”minimikrav” för nätsäkerhet som medlemsstaternas myndigheter själv fastställer. De nationella tillsynsmyndigheterna skall också godkänna planer som systemansvariga tar fram för utbyggnad och modernisering av distributionssystemet så att det håller tillräcklig kapacitet för den gränsöverskridande sammankoppling av eldistributionsnät. Dessa planer skall vidare i en aggregerad form diskuteras av Kommissionen tillsammans med kommittén för tillsynsmyndigheter.[146]

Samtidigt behandlas också ett förslag från Kommissionen där bl.a. ingår att EU skall ta större hänsyn till säkerhetsfrågor vid val av stödprojekt rörande transeuropeiska transport- och energinät.[147]

Informations- och kommunikationstjänster[148]

Området informations- och kommunikationssäkerhet har under de senaste åren genomgått en omfattande utveckling inom EU. eEurope programmet, som utgör en del av Lissabonstrategin, handlar framförallt om att skapa en europeisk IT-arena. På säkerhetssidan nämns bland annat gemensamma specifikationer för ”rörlighet, säkerhet, personlig integritet och användarkontroll”, behovet av att utveckla en ”trust infrastructure” samt målet att skapa ”ett billigare, snabbare och säkrare Internet”. Samtidigt har EU också beslutat om olika delar i ett utvidgat, europeiskt IT-säkerhetsarbetet, inlusive upprättandet av en Byrå för nät- och informationssäkerhet (ENISA).

ENISA skall bland annat förbättra EU:s, medlemsstaternas och näringslivets förmåga att förhindra, ta i tu med och lösa problem som rör nät- och informationssäkerhet. Byrån skall ge stöd i form av råd till Kommissionen och

---

[144] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, FOI juni 2005, sidan 24.
[145] Europeiska Kommissionen: *Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om åtgärder för att trygga elförsörjning och infrastrukturinvesteringar*, KOM(2003)740.
[146] Europeiska Kommissionen: *Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om åtgärder för att trygga elförsörjning och infrastrukturinvesteringar*, KOM(2003)740.
[147] Commission of the European Union: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL determining the general rules for the granting of Community financial aid in the field of the trans-european transport networks and energy and amending Council Regulation (EC) n° 2236/95*, COM(2004)475.
[148] Detta avsnitt bygger framförallt på Pär Eriksson: *Kartläggning av EU:s informationssäkerhetsarbete i första respektive andra pelaren*, FOI MEMO 1017, 2004-11-01.

medlemsstaterna i nät- och informationssäkerhetsfrågor samt främja ett brett samarbete mellan offentliga och privata aktörer (bl.a. bistå Kommissionen och medlemsstaterna i dialogen med industrin). Arbetet sker främst genom att samla in och analysera information som sedan omformas till råd och stöd. Det är fortfarande medlemsstaterna som har det övergripande ansvaret för nät- och informationssäkerheten i respektive land. ENISA får t.ex. inte inkräkta på de nationella regleringsmyndigheternas arbetsuppgifter, vilka bl.a. skall säkerställa de allmänna kommunikationsnätens integritet och säkerhet.

ENISA har till sin hjälp en ”Permanent Stakeholders Group” bestående av experter från industri, akademi och konsumentorganisationer som ger råd i frågor rörande ENISAs verksamhet och som utgör en kontaktpunkt till centrala intressenter.[149]

I mars 2002 antog EU ett ramdirektiv om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster.[150] I detta direktiv ingår att medlemsstaterna skall inrätta nationella regleringsmyndigheter med ansvar att a) främja konkurrensen, b) bidra till utvecklingen av den inre marknaden och c) främja medborgarnas intressen bl.a. genom att säkerställa kommunikationsnätens integritet och säkerhet. Huvudfokus ligger på att skapa en fungerande fri marknad och en god konkurrenssituation. Kommissionen skall samla lämpliga standards för arbetet vilka, om det behövs ur framförallt ett marknads- och konkurrensperspektiv, också kan göras obligatoriska. Det tycks troligt att detta även kan röra sig om standards som handlar om skydd och skyddsnivåer.

2002 antog Europaparlamentet och Rådet ett direktiv om behandling av personuppgifter och integritetsskydd inom telekommunikationssektorn.[151] I detta sägs bl.a. att tjänstetillhandahållaren, om nödvändigt tillsammans med nätoperatören, måste vidta lämpliga åtgärder för att tillse att deras tjänster är säkra.

2005 antogs efter en tre år lång process också ett rambeslut om angrepp mot informationssystem.[152] Syftet är bl.a. att tillnärma olika medlemsstaters lagstiftning och därmed bidra till bekämpning av organiserad brottslighet och terrorism rörande informationssystem. Förslaget innehöll definitioner av olika typer av attacker mot informationssystem, en beskrivning av hotets karaktär och definition av olika typer av brott. Behovet av samarbete underströks. Att åstadkomma

[149] www.enisa.eu.int
[150] EU: *Europaparlamentets och Rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv).*
[151] Europeiska Unionen: *Europaparlamentets och Rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).*
[152] Europeiska Unionen: *Rådets Rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem.*

omfattande skada på informationsinfrastrukturen förklarades som ett terroristbrott redan 2002[153].

Bank-, finans- och försäkringsfunktioner

Det finansiella systemet är intressant ur två aspekter. För det första är det den direkta upprätthållaren av ett av samhällets grundläggande värde – fungerande samhällsekonomi – och måste därför i sin verksamhet kunna hantera påfrestningar som har sitt ursprung i kriser i andra sektorer. För det andra utgör det själv en infrastruktur som kan råka ut för störningar med konsekvenser för samhällsekonomin.

Primärt har det europeiska intresset för den finansiella sektorns regelverk framförallt fötts ur behovet av gemensamma regler för t.ex. säkerheter och penningtransaktioner som en förutsättning för en fungerande inre marknad. De regelverk som finns har inte, vad denna undersökning kunnat visa, haft något fokus på skydd av infrastruktur utan snarast på frågor rörande konkurrens, nivåer på eget kapital för kreditinstitut etc.

Nu pågår emellertid en process att infoga det så kallade ”Basel II” initiativet rörande kapitaltäckning för finansiella institutioner i EU-lagstiftningen. I detta kommer också begreppet ”operativ risk” bli en större del av bedömningen av finansiella institut. Operativ risk innefattar ”risken för förluster till följd av icke ändamålsenliga eller misslyckade processer, mänskliga fel, felaktiga system eller externa händelser”.[154] Detta kan innebära att bl.a. skyddet av bankernas infrastruktur aktualiseras genom att ingå som en del av analysen av bankernas operativa risktagande vid bedömning av kapitaltäckningsgraden.

Kommissionen har tillskapat rådgivande, fristående expertkommittéer rörande olika delar av finanssektorn men övervakning har hittills varit en nationell angelägenhet. De senaste åren har en diskussion pågått i vilken olika former av regleringar och övervakning av ett allt mer transnationellt bank- och finanssystem skall se ut.[155] Samarbete mellan nationella myndigheter snarare än överstatliga kontrollorgan tycks dock troligast.

Intressant är att utvecklingen på det finansiella området drivs genom den öppna så kallade ”Lamfalussy-processen”, vilken består av fyra steg: Gemenskapens lagstiftning sätter en ram, därefter sker en utveckling av tillämpningsbestämmelser av Kommissionen med stöd av en kommitté av medlemsstatsrepresentanter (som t.ex. ”värdepapperskommittén”) vilken skall arbeta öppet bl.a.

---

[153] Europeiska Unionen: *Rådets rambeslut av den 13 juni 2002 om bekämpande av terrorism, 2002/475/RIF*.
[154] Se vidare finansinspektionens hemsida www.fi.se respektive http://europa.eu.int/comm/internal_market/bank/regcapital/index_en.htm#20051027
[155] Commission of the European Union: *Green paper on Financial Services Policy (2005-2010)*, COM(2005)177.

gentemot marknadens aktörer, därefter samverkan mellan nationella övervakningsfunktioner för att tillse harmoniserad tillämpning med stöd av en fristående kommitté med representanter för övervakningsorgan (som t.ex. ”värdepapperstillsynskommittén”) samt slutligen Kommissionens övervakning av efterlevnaden av gemenskapsbestämmelserna.[156] Detta innebär således att såväl lagstiftnings- som implementeringsprocess sker i nära samarbete med marknadens aktörer.

Seveso II, en del av skydd mot farliga ämnen

Rådet antog 1996 det så kallade Seveso II direktivet om skydd mot allvarliga kemiska olyckshändelser.[157] Syftet är att förebygga olyckor samt att minska konsekvenserna för människa och miljö av olyckor i anläggningar för produktion eller lagring av kemiska ämnen.

Enligt direktivet är operatörer av anläggningar med kemiska substanser ansvariga för att upprätta ett handlingsprogram för att förebygga olyckor. För större anläggningar krävs också en säkerhetsrapport innehållande såväl en plan för förebyggande av olyckor som ett säkerhetsledningssystem för att implementera denna plan. Operatörerna skall också upprätta interna räddningsplaner medan myndigheter upprättar, vid behov, räddningsplaner för området utanför anläggningen. Åtgärderna skall syfta till att innesluta och begränsa händelsen och att skydda människa och miljö.

Medlemsstaternas myndigheter skall regelbundet genomföra inspektioner av anläggningar och uppföljning av handlingsprogram och räddningsplaner. För anläggningar där konsekvenserna av en olycka kan sprida sig över gränsen till andra medlemsstater finns också ett informationskrav

Seveso är således ett tvingande direktiv som styr säkerhetsarbetet vid anläggningar med farliga kemiska substanser. Det är inriktat på olyckor, inte händelser styrda av aktör såsom terrorism. Syftet med lagstiftningen är främst att skydda människoliv och miljö. Medlemsstaterna ansvarar för dess genomförande och uppföljning. En kommitté av medlemsstatsrepresentanter diskuterar frågor rörande implementeringen av Seveso II och ger råd om dess praktiska genomförande. Kommissionen genomför inte någon annan uppföljning än att medlemsstaterna är skyldiga att rapportera större olyckor till Kommissionen. För att sprida denna information vidare har ett informationssystem (Major-Accident Reporting System) inrättats.

---

[156] *Final Report of the Committee of Wise Men on The Regulation of European Securities Markets*, Brussels, 2001-02-15.

[157] European Union: *Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances*. Se även www.europa.eu.int/comm/environment/seveso/index.htm.

Kommissionens Joint Research Centre har upprättat Major-Accident Hazards Bureau (MAHB) som ger vetenskapligt och tekniskt stöd till Kommissionen i frågor rörande olyckor med farliga ämnen.[158] MAHB ansvarar för analys av olyckor rapporterade av medlemsstaterna och utvinner lärdomar för att förebygga framtida olyckor. MAHB samlar och utvärderar också riktlinjer, regelverk, ”best practises” etc.

Seveso II utgör bara en del av EU:s verksamhet rörande skydd mot farliga ämnen. Utöver Seveso finns bl.a. ett hälsoskyddsprogram rörande terroristattacker med biologiska eller kemiska substanser, lagstiftning rörande hantering av radiologiska olyckor samt programmet för ”public health” som rör alla aspekter av hälsofrågor, inklusive detektering och behandling av sjukdom beroende på kemiska eller biologiska substanser.[159]

Luft- och sjötransporter

Det finns ett stort antal regelverk rörande transportsystemets säkerhet såväl i betydelsen safety (”funktionssäkerhet”) som security.[160] På sjötransportsidan antogs 2004 en förordning om förbättrat sjöfartskydd på fartyg och i hamnanläggningar vilken inkluderar internationella konventioner om säkerhet i EG-lagstiftningen.[161] Medlemsstaterna ansvarar för genomförandet men Kommissionen genomför inspektioner av medlemsstaternas arbete.

2002 inrättades också en europeisk sjösäkerhetsbyrå, som bl.a. har som uppgift att bistå Kommissionen i utvecklandet av gemenskapslagstiftningen avseende sjösäkerhet och att förse Kommissionen och medlemsstaterna med ”objektiva, tillförlitliga och jämförbara uppgifter och data om sjösäkerhet”. Byrån skall dessutom stödja Kommissionen i dess inspektionsarbete rörande sjöfartsskyddet.[162] De närmare reglerna för dessa inspektioners genomförande skall utvecklas genom kommittologiförfarande. 2002 antogs också ett direktiv om ett övervakningssystem för sjötrafik.[163] Medlemsstaterna har ansvar för systemet och för sanktioner mot dem som bryter mot det.

---

[158] www.mahbsrv.jrc.it

[159] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, FOI juni 2005, sidan 27ff.

[160] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, FOI juni 2005, sidan 26.

[161] ”Europaparlamentets och Rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar”, *Europeiska Unionens Officiella Tidning L129*, 2004-04-29.

[162] ”Europaparlamentets och Rådets förordning (EG) nr 1460/2002 av den 27 juni 2002 om inrättande av en europeisk sjösäkerhetsbyrå”, *Europeiska Unionens Officiella Tidning L208*, 2002-08-05 samt ”Europaparlamentets och Rådets förordning (EG) nr 724/2004 av den 31 mars 2004 om ändring av förordning (EG) nr 1460/2002 av den 27 juni 2002 om inrättande av en europeisk sjösäkerhetsbyrå”, *Europeiska Unionens Officiella Tidning L209*, 2004-04-29.

[163] ”Europaparlamentets och Rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättandet av ett övervaknings- och informationssystem för sjötrafik”, *Europeiska Unionens Officiella Tidning L208*, 2002-08-05.

En särskild förordning med avseende på hamnsäkerhet är när detta skrives i slutstadiet att godkännas av EU:s institutioner.[164] I denna ingår gemensamma säkerhetsregler rörande hamnsäkerhet, en implementeringsmodell för dessa samt en övervakningsmekanism. Medlemsstaterna ansvarar för ett övervakningssystem men Kommissionen skall tillsammans med ansvarig nationell myndighet genomföra inspektioner.

Även på flygsäkerhetsområdet har det skett en omfattande utveckling av EU:s lagstiftning sedan terrordåden 2001. 2002 antogs en förordning om gemensamma skyddsregler som bl.a. innebar införandet av gemenskapsåtgärder för att förhindra olagliga handlingar mot den civila luftfarten.[165] Detta genomförs genom gemensamma standards för luftfartsskydd och övervakningsmekanismer. Varje medlemsstat skall ha ett nationellt säkerhetsprogram, med en myndighet ansvarig för dess samordning och övervakning. Kommissionen genomför, tillsammans med nationell myndighet, inspektioner av såväl medlemsstatens arbete för att genomföra förordningen som av enskilda flygplatsers säkerhetsarbete. Ett antal direktiv för standards, inspektionsrutiner etc. har antagits genom kommittologiförfarande. EU har också inrättat en flygsäkerhetsmyndighet, men denna är inriktad på ”safety” aspekter.

Sjö- och lufttransportområdena kopplar även till utvecklingen av de så kallade trans-europeiska transportnäten. De transportnät som anses ”trans-europeiska” är sådana som bidrar till en väl fungerande inre marknad och till EU:s ekonomiska och sociala sammanhållning.[166] Det handlar således om ”trans-europeiskt” i meningen underbygger EU:s mål. Säkerhetsfrågorna är inte framträdande. I den pågående översynen av stödprogrammen för de trans-europeiska nätverken diskuteras generellt en ökad tyngd på säkerhetsfrågor (safety och security).[167]

Livsmedelssäkerhet och närliggande områden

Inom områdena livsmedelssäkerhet, djurhälsa, djurskydd och växthälsa har EU lagt fast en tämligen långtgående, bindande lagstiftning som bl.a. syftar till att förbättra förmågan att upptäcka och hantera kriser rörande livsmedel. Medlemsstaterna ansvarar för att dessa lagar följs av producenter och andra involverade i

[164] European Union: *Directive 2005/.../EC of the European Parliament and of the Council on enhancing port security*, PE-CONS 3629/05, 2005-07-29.
[165] ”Europaparlamentets och Rådets förordning (EG) nr 2320/2002 av den 16 december 2002 om införande av gemensamma skyddsregler för den civila luftfarten”, *Europeiska Unionens Officiella Tidning L355*, 2002-12-30.
[166] ”Fördraget om upprättandet av Europeiska gemenskapen (Konsoliderad version)”, ”Nicefördraget”, *Europeiska Unionens Officiella Tidning*, C 325 2002-12-24, paragraferna 14, 154 och 158.
[167] Thomas Jönsson, Helén Jarlsvik: *Krisberedskapsmyndigheten och Europeiska Unionen*, FOI-R--1654--SE, FOI juni 2005, sidan 25 samt Commission of the European Union: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL determining the general rules for the granting of Community financial aid in the field of the trans-european transport networks and energy and amending Council Regulation (EC) n° 2236/95*, COM(2004)475.

livsmedelskedjan men Kommissionens kontor för livsmedels- och veterinärfrågor ser till, bl.a. genom inspektioner, att medlemsstaterna tillämpar lagarna.[168]

Europeiska myndigheten för livsmedelssäkerhet (EFSA) är spindeln i ett system för snabb varning (”Rapid Alert System for Food and Feed”, RASFF) samtidigt som Kommissionen har givits befogenheter att agera i krissituationer, inklusive att besluta om att ta livsmedel från marknaden. EFSA, som har ett antal vetenskapliga kommittéer, skall bistå såväl med riskanalyser innan kris uppstått som med råd i krissituationer. EFSA har också i uppdrag att identifiera hot på väg att uppstå, d.v.s. en tidig varningsfunktion.[169]

I någon direkt mening finns inte någon lagstiftning som handlar om att tillse tillgång på livsmedel. Däremot kan hela EU:s jordbrukspolitik ses som ett instrument att tillse att det finns jordbruksproduktion av tillräcklig omfattning i Europa.[170]

Vattenförsörjning och avlopp

EU har givit ut ett antal direktiv rörande vattenkvalitet och delvis också vattenkvantitet. Ett ramverk, en vattenpolicy, läggs i ett direktiv från 2000.[171] Enligt detta skall medlemsstaterna peka ut vattenbassänger (för grund-, yt- och kustvatten) och ange vilka myndigheter som nationellt har ansvar för vattenkvaliteten i dessa. I de fall som vattenbassänger överlappar flera stater skall de berörda medlemsstaterna tillsammans skapa ett ansvarigt organ.

I direktivet ingår att medlemsstaterna i enlighet med föreskrifter i ett antal andra direktiv skall tillse kontroll av vattenkvaliteten, särskilt (men inte enbart) med avseende på vissa farliga ämnen. För varje vattenområde skall upprättas en särskild handlingsplan för att bl.a. tillse en förbättring av vattenkvaliteten i enlighet med EU-direktiv.

Direktivet anger också att alla dricksvattentäkter särskilt skall rapporteras till Kommissionen och att medlemsstaten ansvarar för skydd av dricksvattentäkter. Det finns däremot inte något överstatligt kontrollorgan.

---

[168] www.europa.eu.int/comm/agriculture/foodqual/control_en.htm.

[169] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet.
Information är också hämtat från Kommissionens hemsida för ”Food and Feed Safety”(www.europa.eu.int/comm/food/food/foodlaw/principles/index_en.htm) samt från EFSA:s hemsida (wwww.efsa.eu.int).

[170] Detta är åtminstone ett av de historiska skälen till CAP. Idag är det möjligen inte lika relevant, men används ändå som motiv att försvara CAP. Se t.ex. Commission of the European Union: *The Common Agricultural Policy Explained*, Bryssel 2004, sidan 32.

[171] European Union: *Directive of the European Parliament and of the Council establishing a framework for Community action in the field of water policy*, Brussels, 18 July 2000.

På försörjningssidan anger direktivet att medlemsstaterna senast 2010 skall ha sett över prissättningen på vatten på ett sådant vis att kostnaderna ger konsumenterna tillräckliga incitament för att bruka vattenresurserna effektivt.

På avloppssidan har EU ett regelverk som styr hanteringen av avloppsvatten från urbana områden.[172] I detta ingår också vissa industriavlopp. Fokus ligger på miljöaspekten i ”normal” funktion men det anges även att anläggningarna skall byggas så att de förebygger läckage, klarar av situationer av särskilt kraftiga flöden etc. Medlemsstaterna skall övervaka funktionen hos avloppsverken.

För såväl vatten- som avloppsbestämmelserna är det medlemsstaterna som har ansvaret för uppföljning och övervakning.

[172] European Council: *Council Directive 91/271/EEC of 21 Majy 1991 concerning urban waste-water treatment*.

Bilaga 3. Lagrum för det svenska krisberedskapssystemet

Som en direkt följd av 2002 års proposition antog Riksdagen tre lagar som styr det svenska, offentliga beredskapsarbetet:

1) Lagen om extraordinära händelser i fredstid hos kommuner och landsting (2002:833) vilken reglerar:[173]
    a. kommuners och landstings organisation vid extraordinära händelser (inrättandet av en krisledningsnämnd).
    b. krav på en kommunal plan för hantering av extraordinära händelser.
    c. reglering av hjälp över kommungränserna samt till enskilda medborgare i samband med extraordinära händelser.

2) Förordningen om åtgärder för fredstida krishantering och höjd beredskap (2002:472) enligt vilken:[174]
    a. varje myndighet under Regeringen skall genomföra risk- och sårbarhetsanalyser ”inom sitt ansvarsområde”
    b. särskilt utpekade myndigheter (”samverkansmyndigheterna”) ges särskilt ansvar för att ”planera och vidta förberedelser för att förebygga, motverka och begränsa identiferiad sårberhet och risker”. Samverkansmyndigheterna skall då samverka även med andra berörda myndigheter, sammanslutningar och näringsidkare och särskilt länsstyrelser i deras roll som områdesansvariga myndigheter.
    c. förordningen berör också myndigheternas ansvar vid höjd beredskap, även då med särskilda uppgifter för en utpekad grupp av myndigheter (vilken i stort sammanfaller med tidigare nämnda samverkansmyndigheter) rörande planering och risk- och sårbarhetsanalyser.

3) Förordningen med länsstyrelseinstruktion (2002:864) enligt vilken länsstyrelserna bl.a. skall:[175]
    a. ansvara för åtgärder inom länet i enlighet med 2002:472 och är högsta civila totalförsvarsmyndighet inom ett län.
    b. bevaka att risk- och beredskapshänsyn tas i samhällsplaneringen och främja kommunala risk- och sårbarhetsanalyser.

[173] *Lagen om extraordinära händelser i fredstid hos kommuner och landsting* (2002:833).
[174] *Förordningen om åtgärder för fredstida krishantering och höjd beredskap* (2002:472).
[175] *Förordningen med länsstyrelseinstruktion* (2002:864).

c. samordna planering, inriktning, genomförande och uppföljning av ledningsövningar.

I ”Lag om civilt försvar” (1994:1720) anges dessutom kommunernas och landstingens ansvar inom civilförsvaret, såväl vad gäller förberedelser före som ledning/samordning under en beredskapshöjning.

Utöver dessa lagrum finns också en överenskommelse mellan staten och Kommunförbundet (numera Sveriges kommuner och landsting) som reglerar dels kommuners och landstings krisberedskapsarbete (bl.a. att man skall genomföra risk- och sårbarhetsanalyser, att kommunen har ett geografiskt områdesansvar för krishanteringen, att kommunen skall leda ett krishanteringsråd och att kommunen skall samordna lokala aktörers förberedelser), dels den ersättning staten ger till kommuner och landsting för detta arbete.