En granskning av fyra EU-länders syn på det europeiska programmet för skydd av kritisk infrastruktur (EPCIP)

Madelene Lindström
2008-05-08
Dnr. 1432/2007

KRISBEREDSKAPS
MYNDIGHETEN

Titel: En granskning av fyra EU-länders syn på det europeiska programmet för skydd av kritisk infrastruktur (EPCIP)

Utgiven av Krisberedskapsmyndigheten (KBM)
Upplaga: Finns endast tillgänglig i elektroniskt format

KBM:s diarienummer: 1432/2007

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

Innehåll

SAMMANFATTNING

Det europeiska programmet för skydd av kritisk infrastruktur (European Programme for Critical Infrastructure Protection, EPCIP) kommer att påverka vårt nationella krisberedskapsarbete. Programmet föreslås bestå av tre delar; ett direktiv, ett finansieringsprogram samt ett informations- och varningssystem. Då framförallt direktivet innehåller flera artiklar med bäring på svensk krisberedskap är det av största vikt att analysera och belysa dessa.[1]

Ett sätt att närma sig denna fråga är att studera hur andra EU-länder jobbar med skydd av kritisk infrastruktur, hur de ställer sig till ett direktiv på området, vad de bedömer att direktivet kommer att få för konsekvenser nationellt samt vilka förberedelser som de har vidtagit för en eventuell implementering. I denna rapport studeras Danmark, Finland, Nederländerna och Storbritanniens arbete med skydd av kritisk infrastruktur. Tyngdpunkten i studien ligger i att ta del av ländernas bedömningar av de nationella konsekvenserna till följd av direktivet. Eventuella förberedelser som vidtagits kopplade till kommissionens förslag om inrättandet av ett europeiskt program för skydd av kritisk infrastruktur granskas också. Den övergripande målsättningen är att föreliggande studie ska utgöra en grund för Krisberedskapsmyndighetens (KBM:s) kommande arbete med att ta fram en nationell strategi för skydd av kritisk infrastruktur. Studien ska också kunna användas för att förbereda svenska myndigheter på de förändringar som ett eventuellt direktiv kan komma att medföra i form av nationella anpassningsåtgärder.

En sammanfattning av de granskade ländernas inställning till EPCIP ger vid handen att samtliga länder stödjer det övergripande målet med programmet och betonar vikten av att skydda den kritiska infrastrukturen. Det direkta mervärdet med ett europeiskt program för skydd av kritisk infrastruktur som lyfts fram av de granskade länderna ligger framförallt i möjligheterna till bättre kunskaper om gränsöverskridande verkningar vid störningar i infrastrukturen. Direktivet uppges också kunna bidra till att länder tar ett större ansvar för att skydda sin kritiska infrastruktur som kan ha betydelse även för andra länder. Den till viss del kritiska hållningen till direktivet, som bl.a. Danmark, Nederländerna och Storbritannien har gett uttryck för, handlar delvis om att man vill värna subsidiaritetsprincipen[2] samt vill

[1] Ett direktiv ställer upp vissa krav som den nationella lagstiftningen ska följa, men det är upp till medlemsländerna att utforma reglerna i detalj. Genomförandet av ett direktiv ska göras inom den tidsfrist som direktivet anger men kan se olika ut beroende på hur den nationella lagstiftningen ser ut på området. Det är regeringen som gör den preliminära bedömningen av hur ett direktiv ska införlivas. Ibland motsvarar den svenska lagstiftningen redan direktivets krav och då behöver Sverige inte göra någonting förutom att anmäla detta till kommissionen. Om Sverige behöver stifta en ny lag eller ändra en befintlig lag, så lämnar regeringen en proposition om detta till riksdagen. Ibland kan regeringen själv genomföra direktivet genom att utfärda en förordning, eller genom att uppdra åt en myndighet att utfärda nya föreskrifter. När anpassningen av nationell lagstiftning är klar anmäler regeringen detta till kommissionen. Om Sverige inte har genomfört ett direktiv efter att tidsfristen har gått ut så kan kommissionen dra den svenska staten inför EG-domstolen. Källa: EU-upplysningen

[2] Subsidiaritetsprincipen eller närhetsprincipen som den också kallas innebär att beslut ska fattas på lägsta möjliga beslutsnivå dvs. att medlemsstaterna behåller de befogenheter som de själva kan administrera mest effektivt medan gemenskapen ges de befogenheter

undvika dupliceringar av uppgifter och strukturer. Då flera av de granskade länderna redan bedriver ett omfattande CIP-arbete[3] är man noga med att framhålla vikten av att EPCIP tar hänsyn till vad som redan genomförs av de enskilda länderna.

Sett till artiklarna i direktivet är det framförallt obligatoriet att upprätta säkerhetsplaner s.k. Operator Security Plans (OSP) och att utse sambandsansvariga i säkerhetsfrågor s.k. Security Liaison Officers (SLO) som är problematiskt för Danmark, Nederländerna och Storbritannien. En farhåga som lyftes fram var att man befarade att införandet av nationell lagstiftning av denna typ kan skapa problem i relationen till de privata ägarna och operatörerna av kritisk infrastruktur vilken hittills har byggts på ett frivilligt samarbete.

Vad gäller direktivets obligatorium om inrättandet av säkerhetsplaner uppger samtliga medlemsländer att de flesta ägare och operatörer av kritisk infrastruktur i landet redan är förpliktade att upprätta något som liknar de säkerhetsplaner som föreslås i direktivet. I många av de granskade länderna har man på senare tid också inrättat rådgivningscenter där man bl.a. bistår ägare och operatörer vid upprättandet av säkerhetsplaner. I Storbritannien har exempelvis alla ägare och operatörer av nationell kritisk infrastruktur tillgång till kostnadsfria ”security advisers”. I Nederländerna och Finland tillhandahåller det nationella rådgivningscentret för skydd av kritisk infrastruktur (NAVI)[4] respektive Försörjningsberedskapscentralen (FBC) motsvarande tjänster.

Samma sak gäller för utpekandet av sambandsansvariga i säkerhetsfrågor där det från flera håll framkom att de flesta ägare och operatörer av kritisk infrastruktur redan har någon som är utpekad som ansvarig för säkerhetsfrågor även om dessa inte benämns just ”Security Liaison Officers”.

Vad gäller rollen som kontaktpunkt i frågor som rör skydd av europeisk kritisk infrastruktur (s.k. CIP-Contact Point) är det dominerande svaret att man inom de granskade länderna inte avser att utse någon ny myndighet för denna uppgift. I Storbritannien är det exempelvis Inrikesdepartementet som innehar denna roll i dagsläget och den brittiska inställningen är att detta ministerium även i fortsättningen ska ha den rollen. Om funktionen däremot skulle bli mer teknisk till sin karaktär så avser man att överväga att eventuellt flytta denna funktion till the Centre for the Protection of National Infrastructure (CPNI) då dessa besitter den tekniska kompetensen.

En slutsats är att samtliga av de granskade länderna gör bedömningen att ett direktiv inte kommer att påverka deras nuvarande arbetssätt kring skyddet av den kritiska infrastrukturen nämnvärt. Den dominerande uppfattningen är att en implementering av direktivet främst kommer att

---

som medlemsstaterna inte kan utöva på tillfredsställande sätt. Inom EU infördes principen genom Maastrichtfördraget, som trädde ikraft i november 1993.

[3] Skydd av kritisk infrastruktur och den engelska vedertagna förkortningen Critical Infrastructure Protection (CIP) kommer att användas synonymt i texten.

[4] Nationaal Adviescentrum Vitale Infrastructuur.

handla om en lagstiftningsfråga. Baserat på bedömningen att de flesta ägare och operatörer av kritisk infrastruktur redan har något som motsvarar de säkerhetsplaner och sambandsansvariga i säkerhetsfrågor som direktivet föreskriver förväntar sig heller inte de granskade länderna att en implementering av direktivet kommer att medföra några omfattande kostnader. Detta gäller såväl för offentliga aktörer som för de privata ägarna och operatörerna av utpekad europeisk kritisk infrastruktur. Från brittiskt håll framhölls dock att direktivet i sig ändå kan medföra en kostnad för ägarna och operatörerna av utpekad europeisk kritisk infrastruktur då det kan finnas ett behov för dessa att vidta åtgärder för att säkerställa att de följer eventuell ny lagstiftning.

Samtliga av de granskade länderna har haft workshops och möten med departement och centrala myndigheter som kommer att beröras av direktivet. Som en följd av bedömningen att ett direktiv inte kommer att påverka det befintliga arbetet nämnvärt har man dock inte vidtagit några andra förberedelser för en eventuell implementering av direktivet. Av de granskade länderna är det endast Storbritannien, och i viss mån Nederländerna, som har genomfört en nationell konsekvensanalys av direktivet. Inom ramen för den brittiska konsekvensanalysen tittade man bl.a. på vad som redan görs nationellt, hur man skulle kunna genomföra direktivet och vilka konsekvenser det eventuellt skulle kunna få. I Storbritannien har man också gjort en preliminär uppskattning av vad som eventuellt skulle kunna utpekas som europeisk kritisk infrastruktur (ECI). Bedömningen är att det i hela Storbritannien kan komma att handla om drygt 10 stycken utpekade ECI och den brittiska förhoppningen är att man, efter att den slutliga definitionen fastställts, totalt inom EU inte ska identifiera mer än drygt 100 ECI. De övriga granskade länderna har inte gjort någon motsvarande bedömning av potentiella ECI med hänvisning till att definitionen ännu inte är färdigförhandlad. Från finskt håll framhåller man dock att situationen i Norden skiljer sig betydligt från den nere på kontinenten där länderna är mer sammanlänkade.

Den övergripande slutsatsen som dras i studien är att de resonemang som förts fram av de nationella företrädarna tyder på att man i samtliga av de granskade medlemsstaterna tycks ta implementeringskonsekvenserna med ro. En analys av studiens resultat indikerar vidare att de granskade medlemsstaterna som argumenterat emot direktivet tycks ha byggt upp sina ställningstaganden på principiella argument om vad som ska hanteras på nationell nivå och vad som ska skötas på EU-nivå snarare än någon bedömning av att ett direktiv skulle medföra omvälvande och betydande förändringar vilka skulle bli svåra att genomföra i förhållande till det befintliga nationella arbetet.

Vägen framåt

Vad gäller den fortsatta nationella processen till följd av ett eventuellt direktiv på området förefaller en viktig del vara att löpande hålla berörda aktörer - såsom sektorsmyndigheter, departement och ägarna/operatörerna av europeisk kritisk infrastruktur - informerade och delaktiga i arbetet genom exempelvis workshops och möten. Utöver detta kan tre mer

specifika spår och processer identifieras som det framtida nationella arbetet bör kretsa kring:

- *Nationell inventering av potentiell europeisk kritisk infrastruktur*

En central första uppgift förefaller vara att identifiera potentiella ECI i landet för att utröna hur direktivet kommer att påverka Sverige nationellt. Här kan man exempelvis tänka sig att undersöka huruvida ägare och operatörer av potentiella ECI i landet redan har något liknande de säkerhetsplaner och sambandsansvariga i säkerhetsfrågor som direktivet stipulerar. Genom ett sådant agerande kan man få en indikation på vilka områden förändringar är att vänta samt hur omfattande dessa förändringar kan förväntas bli. Ett ingångsvärde här skulle kunna vara att utgå ifrån de av kommissionen tre prioriterade sektorerna transporter, energi och informations- och kommunikationsteknologier.

- *Analys av organisatoriska effekter tillföljd av ett direktiv på området*

Efter en nationell inventering av potentiell europeisk kritisk infrastruktur är en naturlig fortsättning att titta närmare på vilka organisatoriska effekter ett direktiv kan få på det befintliga nationella arbetet. Det kan exempelvis handla om en generell konsekvensanalys där man tittar på hur sakområdena och de befintliga arbetsprocesserna kommer att påverkas till följd av ett direktiv dvs. ansvarsfördelningen mellan ägare och operatörer av ECI i förhållande till berörda sektorsmyndigheter, relationen mellan Regeringskansliet och den nya myndigheten för samhällets skydd och beredskap samt EPCIP:s inverkan på befintlig lagstiftning, finansiering och varningssystem.

- *Framtagande av ett nationellt CIP-program*

Ett tredje spår som är nära sammankopplat och kan bygga på de första två punkterna är framtagandet av en nationell CIP-strategi. Här kan man tänka sig att implementeringen av EPCIP endast utgör en del av det mycket bredare arbetet med att ta fram en nationell CIP-strategi där man utöver europeisk kritisk infrastruktur även identifierar nationell kritisk infrastruktur och lägger upp en övergripande plan för hur man ska jobba med att skydda denna. Inom ramen för det europeiska programmet för skydd av kritisk infrastruktur uppmanas t.ex. medlemsstaterna att, på frivillig basis, inrätta eller utveckla nationella program för skydd av kritisk infrastruktur baserat på EPCIP.

Fackuttryck/förkortningar

CBRN	Kemiska, biologiska, radiologiska och nukleära (hot och risker)
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIWIN	Critical Infrastructure Warning and Information Network
ECI	European Critical Infrastructure
EPCIP	European Programme for Critical Infrastructure Protection
EU	Europeiska unionen
KBM	Krisberedskapsmyndigheten
OSP	Operator Security Plan
PPP	Public-Private Partnership
ProCiv	Civil protection working party
SLO	Security Liaison Officer

1 INLEDNING

Internationellt krisberedskapssamarbete bedrivs idag i såväl bilaterala som multilaterala fora. Bilateralt samarbetar Sverige kring krisberedskapsfrågor i den nordiska kretsen, samt med ett flertal EU-medlemmar, USA och Kanada medan multilateralt krisberedskapssamarbete främst sker inom ramen för EU och Nato samt dess partnersamarbete EAPR/PFF[5]. Då EU intar en särställning bland de multilaterala samarbetsfora som Sverige deltar i på krisberedskapsområdet och samarbetet förväntas ytterligare fördjupas och formaliseras finns ett stort behov av att öka kunskapen om EU:s framväxande krisberedskapsarbete och dess nationella implikationer.

En viktig fråga inom EU:s krisberedskapsarbete som kommer att påverka vårt nationella krishanteringssystem framöver är det europeiska programmet för skydd av kritisk infrastruktur (EPCIP). Programmet är för närvarande under förhandling men föreslås bestå av tre huvuddelar; ett direktiv, ett finansieringsprogram samt ett informations- och varningssystem (CIWIN)[6]. Samtidigt som EU-samarbeten tillför mycket till det gemensamma europeiska krisberedskapsarbetet innebär det också åtaganden som får konsekvenser på den nationella arenan. Då framförallt direktivet innehåller flera artiklar med bäring på svensk krisberedskap är det av största vikt att analysera och belysa vilka konsekvenser detta kommer att få för den svenska krisberedskapen.[7]

Krisberedskapsmyndigheten (KBM) och övriga myndigheter med ett särskilt ansvar för krisberedskapen ska verka för att EU-samarbetet blir en integrerad verksamhet i samhällets krisberedskap. Det framgår av förordningen (2006:942) om krisberedskap och höjd beredskap där 11 § anger att myndigheter med ett särskilt ansvar för krisberedskapen ska ”beakta det samarbete som sker inom Europeiska unionen och internationella frågor i forum som rör samhällets krisberedskap”.[8] Ett sätt att närma sig frågan kring hur EPCIP kommer att påverka det befintliga nationella arbetet på området är att ta del av de lösningar som finns rörande skydd av kritisk infrastruktur i andra EU-länder, studera hur de ställer sig till ett direktiv på området, vad de bedömer att direktivet kommer att få för konsekvenser nationellt samt vilka förberedelser de har vidtagit för en eventuell implementering av programmet. Att titta på länder som är ”lika” Sverige storleksmässigt och utvecklingsmässigt på

[5] Euroatlantiska partnerskapsrådet (EAPR); Partnerskap för fred (PFF)
[6] Critical Infrastructure Warning and Information Network (CIWIN)
[7] Ett direktiv ställer upp vissa krav som den nationella lagstiftningen ska följa, men det är upp till medlemsländerna att utforma reglerna i detalj. Genomförandet av EU-direktiv ska göras inom den tidsfrist som direktivet anger men kan se olika ut beroende på hur den nationella lagstiftningen ser ut på området. Det är regeringen som gör den preliminära bedömningen av hur ett direktiv ska införlivas. Ibland motsvarar den svenska lagstiftningen redan direktivets krav och då behöver Sverige inte göra någonting förutom att anmäla detta till kommissionen. Om Sverige behöver stifta en ny lag eller ändra en befintlig lag, så lämnar regeringen en proposition om detta till riksdagen. Ibland kan regeringen själv genomföra direktivet genom att utfärda en förordning, eller genom att uppdra åt en myndighet att utfärda nya föreskrifter. När anpassningen av nationell lagstiftning är klar anmäler regeringen detta till kommissionen. Om Sverige inte har genomfört ett direktiv efter att tidsfristen har gått ut så kan kommissionen dra den svenska staten inför EG-domstolen. Källa: EU-upplysningen
[8] Förordningen (2006:942) om krisberedskap och höjd beredskap 11 §.

krisberedskapsområdet innebär exempelvis att vi också har samma utgångsläge och står inför liknande utmaningar vid en eventuell implementering av ett direktiv. Genom att studera EU-länder som är ledande på området får vi dessutom möjligheter att ta del av *best practices*.

Studien ska ses som ett första steg i det kommande arbetet med att utveckla en nationell strategi för arbetet med skydd av kritisk infrastruktur. Studiens målgrupp är i första hand KBM, de myndigheter som är utpekade i förordningen om krisberedskap och höjd beredskap samt den nya myndigheten för samhällets skydd och beredskap.[9]

1.1 Syfte

Denna studie genomförs på uppdrag av KBM. I KBM:s sektorsövergripande samordningsansvar för svensk krisberedskap ingår bl.a. att förse det svenska krishanteringssystemet med relevant kunskap. Då direktivet kopplat till det europeiska programmet för skydd av kritisk infrastruktur innehåller flera artiklar med bäring på svensk krisberedskap är det av största vikt att analysera och belysa vilka konsekvenser EPCIP får för den svenska krisberedskapen.

Mot denna bakgrund är syftet med denna rapport att inhämta kunskap om hur Danmark, Finland, Nederländerna och Storbritannien arbetar med skydd av kritisk infrastruktur (CIP)[10]. Mer specifikt kommer följande frågeställningar att belysas:

- Hur arbetar landet med skydd av kritisk infrastruktur?
- Hur ställer man sig till det europeiska programmet för skydd av kritisk infrastruktur?
- Hur bedömer man att EPCIP kommer att påverka det nationella arbetet kring skydd av kritisk infrastruktur?
- Vilka nationella förberedelser har vidtagits för att förbereda för en eventuell implementering av det europeiska programmet för skydd av kritisk infrastruktur?

Tyngdpunkten i studien är att ta del av ländernas bedömningar av de nationella konsekvenserna samt eventuella förberedelser som vidtagits kopplade till kommissionens förslag om inrättandet av ett europeiskt program för skydd av kritisk infrastruktur.

1.2 Disposition och läsanvisningar

I kapitlet ”Metod, material och avgränsningar” redovisas hur studien genomförts, bakomliggande metodansatser och överväganden samt

[9] Sjöstrand ”Alltid redo! En ny myndighet mot olyckor och kriser” SOU 2007:31. Utredningen föreslår att Krisberedskapsmyndigheten (KBM), Räddningsverket (SRV) och Styrelsen för psykologiskt försvar (SPF) ska slås ihop till en ny myndighet för samhällets skydd och beredskap.

[10] Skydd av kritisk infrastruktur och den engelska vedertagna förkortningen Critical Infrastructure Protection (CIP) kommer att användas synonymt i texten.

avgränsningar och begrepp som är centrala för studien. Fokus ligger här på de jämförelsepunkter som strukturen i respektive landgenomgång baseras på. Kapitel tre beskriver översiktligt EU:s krishanteringsarbete samt ger en bakgrund till EU:s arbete med skydd av kritisk infrastruktur. Inom ramen för detta kapitel görs även en kort redogörelse för direktivförslaget med fokus på de delar som föreslås vara obligatoriska. Efter en genomgång av de centrala artiklarna i direktivet avslutas kapitlet med att ge en översiktlig bild av förhandlingarnas nuvarande status och utestående frågor.

I arbetet med att ta fram en nationell strategi för skydd av kritisk infrastruktur har en kartläggning av andra medlemsstaters arbete på området en central roll. Hur arbetar man med skydd av kritisk infrastruktur i Danmark, Finland, Nederländerna och Storbritannien? Hur ser man på EPCIP? Vad bedömer man att direktivet kommer att få för konsekvenser på nationell nivå? Och vilka förberedelser görs för en eventuell implementering? Kapitel fyra till sju syftar till att utifrån fyra fallstudier ge en överblick av några utvalda EU-länders arbete med skydd av kritisk infrastruktur med fokus på deras behandling av EPCIP. Avsnitten beskriver bland annat när landet ifråga började arbeta med skydd av kritisk infrastruktur, vad man definierar som kritisk infrastruktur, hur ansvars- och ledningsstrukturer ser ut, vilken roll de lokala myndigheterna, departementen och andra centrala aktörer har samt hur CIP-åtgärder finansieras. Därefter redogörs för landets inställning till direktivet, vilka konsekvenser man bedömer att det kommer att få på nationell nivå och vilka förberedelser som vidtagits för en eventuell implementering. Varje landavsnitt avslutas slutligen med en kort sammanfattning samt en lista över kontaktvägar till departement och myndigheter som har en central roll i arbetet med skydd av kritisk infrastruktur i landet samt viktigare nationella dokument och rapporter på CIP-området.[11] I det åttonde kapitlet presenteras avslutningsvis rapportens resultat för att slutligen åtföljas av en diskussion kring vägen framåt i kapitel 9.

För den läsare som snabbt vill få en sammanfattning av studiens resultat föreslås att denne tar del av kapitel ett och två, som ger en bakgrund till studien och viktiga ingångsvärden för att kunna värdera de resultat som presenteras i rapporten, samt kapitel åtta och nio som ger en sammanfattning av de studerade ländernas arbete på området och lyfter fram studiens huvudresultat.

[11] I samtliga fall gäller dock att det inom olika sakpolitikområden finns insatser som kan ses som CIP medan det finns ytterst få dokument som e x p l i c i t fokuserar på CIP.

2 METOD, MATERIAL OCH AVGRÄNSNINGAR

Det europeiska programmet för skydd av kritisk infrastruktur består lite förenklat av tre huvuddelar; ett direktivförslag, ett finansieringsprogram och ett förslag till informations- och varningssystem (CIWIN) men då direktivet kan sägas utgöra huvuddelen av programmet behandlar studien endast denna del.

En annan central avgränsning för studien är att uppdraget utgår ifrån EU:s framväxande politik för skydd av kritisk infrastruktur såsom den uttrycks i liggande dokument men då någon enighet ännu inte uppnåtts kring direktivet går det i skrivande stund inte att uttala sig om hur programmet i detalj slutligen kommer att utformas (och följaktligen inte heller exakt vilka åtaganden som kan väntas på nationell nivå).

Länderna i studien är valda utifrån tre kriterier; (1) sådana som är ledande på området i en europeisk kontext (framförallt Nederländerna och Storbritannien) vilket innebär att möjligheterna att ta del av best practices är goda och (2) sådana som är ”lika” Sverige storleksmässigt och utvecklingsmässigt på krisberedskapsområdet (exempelvis Danmark och Finland). Genom att studera länder vars krisberedskapsarbete är uppbyggt på ett liknande sätt som det svenska har vi också samma utgångsläge och står inför liknande utmaningar vid en eventuell implementering av ett direktiv. (3) Det tredje kriteriet täcker in alla dessa länder då det helt enkelt utgått ifrån länder som ligger nära oss rent geografiskt och med vilka vi följaktligen kan komma att behöva samarbeta med kring eventuella gemensamma utpekade ECI.[12] Det hade vidare varit fruktsamt att närmare studera utomeuropeiska stater som är ledande på området (exempelvis USA, Kanada eller Australien) men med tanke på den begränsade tiden var detta inte möjligt och då de inte direkt berörs av EPCIP var detta inte heller prioriterat.

Det första analyssteget i studien består i att övergripande beskriva hur respektive land jobbar med skydd av kritisk infrastruktur. Redan i tidigare rapporter på området har det konstaterats att det är svårt att finna forskning som studerar sektorsövergripande system för skydd av kritisk infrastruktur. Forskare har spekulerat i att några av anledningarna till detta kan ha att göra med att stater av tradition och arv så starkt styr hur man arbetar med skydd av kritisk infrastruktur att jämförande analyser blir svåra eller att de existerande systemen bygger på politiska beslut och att det därmed inte finns något intresse av att finansiera forskning som möjligen skulle visa att dessa beslut inte alltid lett till optimala strukturer. En annan teori är att forskare i allmänhet är mer intresserade av specifika sakområden snarare än policy- och sektorsövergripande frågor.[13]

Med hänvisning till just den begränsade forskningen kring jämförelser av arrangemang för skydd av kritisk infrastruktur på systemnivå har tidigare

[12] En efterföljande studie hade även kunnat inkludera övriga stora medlemsstater som t.ex. Tyskland och Frankrike då dessa kan komma att få ett stort inflytande på programmets slutliga utformning.
[13] Eriksson, Barck-Holst (2005), s.17f

forskare ofta valt att approchera frågan genom att bryta ner CIP-begreppet till ett antal jämförelsepunkter. Med utgångspunkt i Eriksson och Barck-Holsts studie ”Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys” har följande punkter valts ut för att beskriva respektive lands CIP-arbete inom ramen för denna studie; (1) vad utgör kritisk infrastruktur i det studerade landet?, (2) hur identifierar man kritisk infrastruktur?, (3) mot vad anser man att kritisk infrastruktur ska skyddas?, (4) hur ska detta skyddet utformas?, (5) vem ansvarar för skyddet av kritisk infrastruktur? samt (6) hur finansieras skydd av kritisk infrastruktur?[14] Vad gäller kopplingen till EPCIP kommer undersökningen att utgå ifrån (7) hur landet ställer sig till ett direktiv för skydd av kritisk infrastruktur?, (8) hur man bedömer att ett direktiv kommer att påverka det nationella arbetet med skydd av kritisk infrastruktur och slutligen (9) om några förberedande åtgärder har vidtagits för en eventuell implementering av ett direktiv på området. Denna studies begränsade omfattning innebär dock att det inte är möjligt att diskutera de olika faktorerna i detalj utan dessa punkter ska snarare ses som en hjälp för att ge en översiktlig beskrivning av de nationella arrangemangen för skydd av kritisk infrastruktur. Nedan ges en kort genomgång av respektive jämförelsepunkt.

Vad är kritisk infrastruktur?

De senaste åren har såväl enskilda länder som internationella organisationer producerat rapporter om vad som är att betrakta som kritisk infrastruktur och hur man bäst ska skydda denna. Under en lång tid har de största delarna av det som uppfattats som kritisk infrastruktur varit informationsrelaterat. Begreppet skydd av kritisk infrastruktur (CIP) innehåller dock utöver skydd av informationsinfrastrukturer (CIIP) även andra delar av den viktiga samhällsinfrastrukturen.[15]

Tidigare studier av vad olika länder nationellt inkluderar i begreppet kritisk infrastruktur har visat att olika länder har olika men liknande definitioner. Det vanligaste är vida definitioner och tolkningar som inkluderar tekniska nätverk och grundläggande samhällsverksamheter som t.ex. finanssystem och hälsovård.[16]

Utifrån ländernas definitioner har forskare identifierat tre typer av strukturer som ett land kan ha på sitt nationella CIP-arbete. Enligt forskare kan en CIIP-approach, som namnet antyder, härledas till att det främst är skyddet och säkerheten av informations- och kommunikationsteknologier som står i fokus. Här är skyddet av de fysiska komponenterna försäkrad i separata organisatoriska ramverk. Funktioner och kompetenser relaterade till skydd av kritisk infrastruktur är i sin tur uppdelade mellan olika organ och försök görs också till att integrera den privata sektorn i alla sektorer. Den andra s.k. all-hazards approachen kännetecknas av en bred syn på hot och risker

[14] Eriksson, Barck-Holst (2005) s.9ff.

[15] Skydd av kritisk informationsinfrastruktur (CIIP) används för att uttrycka specifikt skyddet av de informationsrelaterade infrastrukturerna skilt från övriga delar av samhällets kritiska infrastruktur. CIP är alltså i regel det bredare begreppet medan CIIP innefattar en central del av denna. I vissa av de undersökta länderna koncentreras verksamheten till största delen på den informationstekniska infrastrukturen dvs. CIIP.

[16] Se bilaga I för en sammanställning av några utvalda länder och organisationers definitioner av kritisk infrastruktur.

vilket innebär att såväl kritisk IT-infrastruktur som det fysiska skyddet av kritisk infrastruktur betonas. Här är det fysiska skyddet en del av den nationella civila försvarsmodellen och den centrala koordinationen och strategiorganen är simultana kompetenscenter i IT-säkerhet, civilt försvar och kriskontroll. Här finns m a o ingen klar uppdelning mellan de olika komponenterna. I denna struktur har ofta försvarsministerierna en framstående roll att koordinera arbetet. Den tredje approachen är lite speciell och kan bortses ifrån i denna studie då den bara kan skönjas i det kinesiska arbetet med skydd av kritisk infrastruktur. Här finns inget samarbete mellan den privata och den offentliga sektorn och modellen handlar egentligen mer om att bevara det befintliga styrelseskicket och organen som representerar statsintresset än att skydda den nationella kritiska infrastrukturen.[17]

Hur identifierar man kritisk infrastruktur?
Tidigare forskare har sammanfattat att vad som utgör kritisk infrastruktur kan ses utifrån ett symbol- och/eller ett systemperspektiv. Lite förenklat kan man säga att medan symbolperspektivet fokuserar på den kritiska infrastrukturens egenvärde för samhället så utgår systemperspektivet ifrån en kedjeuppbyggnad där en infrastruktur är kritisk pga. att den stödjer andra infrastrukturer i samhället. Kopplat till detta kan graden av systematik vid själva identifieringen av kritisk infrastruktur variera mellan stater (och sektorer) och en annan central jämförelsepunkt är därmed hur den kritiska infrastrukturen har identifierats och av vem. Här handlar det t.ex. om huruvida identifieringsprocessen skett nedifrån och upp eller uppifrån och ned samt i vilken grad privata aktörer deltagit i identifieringsprocessen.[18]

Mot vad anser man att kritisk infrastruktur ska skyddas?
Då de identifierade hoten ofta är grundläggande för hur skyddet av den kritiska infrastrukturen utformas är hotbilden en annan viktig jämförelsefaktor. Vad den kritiska infrastrukturen ska skyddas mot kan enligt Eriksson och Barck-Holst dels bedömas utifrån vilka konsekvenser det får av att något inträffar men också utifrån sannolikheten att det inträffar. Författarna framhåller att det i Europa generellt är de aktörsoberoende hoten som jordbävningar, stormar och översvämningar som har störst sannolikhet att inträffa men att det trots det är de aktörsstyrda händelserna som terrorism som har kommit i fokus vid uppbyggnaden av skyddet för den kritiska infrastrukturen. Andra faktorer som enligt författarna kan påverka hotbedömningar är att olika länder lever under delvis olika hotbilder och att olika sektorer kan värdera hoten olika. Det senare har exempelvis betydelse för om det finns en centralt formulerad hotbild eller om varje infrastruktursektor har utvecklat en egen hotbild. Ytterligare en faktor som avgör hur skyddet av den kritiska infrastrukturen ska utformas är huruvida man gör en åtskillnad mellan normala och extraordinära händelser.[19]

[17] Brömmelhörster, J; Fabry, S; Wirtz, N; (2003) Critical Infrastructure Protection: Survey of World-Wide Activities.
[18] Eriksson, Barck-Holst (2005) s.21-24
[19] Eriksson, Barck-Holst (2005) s.25f

Hur ska skyddet av kritisk infrastruktur utformas?
Enligt Eriksson och Barck-Holst kan skyddets utformning handla om vilket slags insatser för skydd av kritisk infrastruktur som prioriteras och vilken fas av skyddsarbetet man lägger tonvikt på. Skyddsarbetet av kritisk infrastruktur kan exempelvis delas in i fyra olika faser (1) förebyggandefasen, (2) beredskapsfasen, (3) den faktiska hanteringen samt (4) återhämtningsfasen. Vidare påverkar det även på denna punkt huruvida man gör en skillnad mellan normala och extraordinära händelser. I Sverige görs exempelvis en skiljelinje mellan en basförmåga att hantera vardagliga händelser samt en förstärkt förmåga att hantera stora fredstida kriser av större dignitet eller väpnande angrepp medan man inom EU inte gör denna uppdelning utan snarare riktar in sig på hela spektrumet av potentiella olyckor och kriser.[20]

Vem ansvarar för skyddet av kritisk infrastruktur?
Vem som ansvarar för skyddet av kritisk infrastruktur handlar om hur ansvarsfördelningen ser ut mellan nationell, regional och lokalnivå samt uppdelningen mellan det privata och det offentliga. En annan viktig fråga är huruvida skydd av kritisk infrastruktur är en del av en övergripande strategi för samhällets säkerhet eller om den utgör ett ensamstående politikområde. Enligt Eriksson och Barck-Holst behöver det här inte handla om något allt eller inget och om att gå så långt som att hävda att de flesta stater bortsett från USA inte har någon övergripande strategi för skydd av kritisk infrastruktur utan det kan snarare handla om att beskriva variationerna i omfång mellan olika staters strategier (exempelvis det sektorsövergripande CIP-systemets grad av centralisering/decentralisering).[21]

Hur finansieras skydd av kritisk infrastruktur?
Finansiering av CIP-åtgärder kan i sin tur ske på tre olika sätt, (1) ägare och operatörer finansierar skyddet av sin kritiska infrastruktur (detta kan i sin tur vara frivilligt eller lagstadgat), (2) ansvarig statlig nivå tar in avgifter som används för att finansiera skyddsinsatser eller (3) genom att ansvarig statlig nivå anslagsfinansierar åtgärder för skydd av kritisk infrastruktur.[22]

Efter en beskrivning av respektive lands arbete med skydd av kritisk infrastruktur utifrån ovan angivna jämförelsepunkter består det andra analyssteget i att försöka teckna en bild av respektive lands inställning till det direktiv om en kartläggning och klassificering av europeisk kritisk infrastruktur som för närvarande förhandlas. Här kommer jämförelserna att beröra vad man ser för mervärde med en gemensam EU-ram på området samt vilka artiklar som eventuellt kan framstå som problematiska. Kopplat till detta utgår beskrivningarna av hur respektive land bedömer att ett direktiv kommer att påverka det nationella arbetet med skydd av kritisk infrastruktur ifrån vad man uppskattar att en implementering får för konsekvenser i form av budgetära merkostnader, lagstiftningsändringar samt förändringar i den privatoffentliga samverkan.

[20] Eriksson, Barck-Holst (2005) s.26ff.
[21] Eriksson, Barck-Holst (2005) s.27
[22] Eriksson, Barck-Holst (2005) s.30

Det tredje och sista analyssteg består slutligen i att granska vilka förberedande åtgärder som vidtagits för en eventuell implementering av ett direktiv på området. Det handlar delvis om huruvida länderna ifråga gjort någon nationell konsekvensanalys, om nationella arbetsgrupper har inrättats för ändamålet samt huruvida några organisatoriska förändringar har vidtagits som en direkt följd av genomförandet av ett eventuellt direktiv på området. Även om de olika länderbeskrivningarna i denna rapport i viss mån skiljer sig åt när det gäller de utvecklingstendenser som blir belysta är ansatsen i samtliga kapitel att teckna en lägesbild över centrala delar av det förberedelsearbete som pågår i de studerade länderna inför en eventuell implementering av ett direktiv på området.

Material

Bakgrunden till beskrivningen av EU:s arbete rörande skydd av kritisk infrastruktur har tagit sin utgångspunkt i tidigare rapporter samt offentligt material från svenska myndigheter och EU. Materialet från EU består till största delen av primärmaterial från EU:s institutioner och då i synnerhet generaldirektoratet för frihet, rättvisa och säkerhet (GD JLS) som äger EPCIP-frågan. Avsnittet som behandlar direktivets innehåll grundar sig till stor del på kommissionens öppna grunddokument som finns att tillgå via Internet samt mötesanteckningar och direktivsutkast från möten i rådsarbetsgruppen ProCiv.[23]

Merparten av materialet om organiseringen av krisberedskapsarbetet i respektive land kommer från KBM:s framtagna länderunderlag. Förutom de specifika referenser som lämnas i notform avslutas varje kapitel med ett antal hänvisningar till webbadresser och/eller annan litteratur med ytterligare information kring krishanteringssystemet i det aktuella landet. Läsaren bör erinra sig om att landgenomgångarna inte ska ses som heltäckande utan snarare som en hjälp och grund för att placera studiens övergripande syfte – att ta del av ländernas bedömningar av de nationella konsekvenserna samt eventuella förberedelser som vidtagits kopplade till direktivet ifråga - i sin rätta kontext. För en heltäckande analys av ett lands CIP-politik och CIP-arbete hade exempelvis även en genomgång av de sektorer som inkluderas i den nationella definitionen av kritisk infrastruktur varit nödvändig. Inom ramen för denna begränsade studie har det dock inte varit möjligt att gå närmare in på de olika sakpolitikområdena.

Då endast en begränsad krets i form av de närmast berörda departementen och myndigheterna har inblick i de aspekter som utgör studiens huvudfokus utgör intervjuer den huvudsakliga källan i denna studie. En risk med intervjuer är att de intervjuades svar kan spegla en personlig uppfattning snarare än landets officiella linje. I de flesta fall har dock den information och de argument som framkommit bekräftats vid andra intervjuer och/eller i skriftliga källor. Utöver intervjuer baseras exempelvis framställningen av medlemsländernas ståndpunkter till EPCIP också på den skriftliga återrapporteringen från möten i rådsarbetsgruppen ProCiv där respektive lands delegater återkommande har förmedlat landets officiella linje.

[23] ProCiv står för the Working Party on Civil Protection (rådsarbetsgruppen för skydd och beredskap).

För att få information om eventuella nationella förberedelser till följd av det europeiska programmet för skydd av kritisk infrastruktur har information huvudsakligen inhämtats genom telefonintervjuer med tjänstemän på ansvarigt departement. Då varken danska Beredskabscentralen (BRS) eller det danska Försvarsdepartementet har haft möjlighet att delta i studien bygger dock avsnittet om den danska inställningen till direktivet endast på landets officiella dokument samt den skriftliga återrapporteringen från möten i rådsarbetsgruppen ProCiv.

Vid granskningen av vilka konsekvenser man bedömer att EPCIP kan komma att få på nationell nivå har studien främst fokuserat på de delar av direktivet som kommer att bli bindande. Med anledning av den begränsade tid som stod till förfogande för studien bedömdes det inte vara möjligt att göra intervjuer med företrädare inom de olika sektorerna och/eller ägare/operatörer av kritisk infrastruktur. Vid en efterföljande fördjupningsstudie skulle exempelvis de av kommissionen tre prioriterade sektorerna transporter, informations- och kommunikationsteknologier samt energi med fördel kunna studeras närmare på detta sätt.

3 EU:S ARBETE MED SKYDD AV KRITISK INFRASTRUKTUR

3.1 Bakgrund

Under 2000-talet är det framförallt fyra övergripande processer som har stått ut på säkerhetsområdet inom EU; (1) Lissabonfördraget - som lägger ett ramverk för EU-samarbetet på säkerhetsområdet, (2) utvecklandet av en europeisk säkerhetsstrategi - som fokuserar på EU:s externa säkerhetsarbete, (3) Haagprogrammet - som fokuserar på EU:s inre säkerhet samt (4) handlingsplanen för terrorismbekämpning och solidaritetsklausulen. Även om samtliga av dessa processer berör området skydd av kritisk infrastruktur är det endast två övergripande processer som explicit är inriktade på skydd av kritisk infrastruktur nämligen EU:s arbete för att förbättra förmågan att möta och hantera terrorism och kommissionens förslag om inrättandet av ett europeiskt program för skydd av kritisk infrastruktur.[24]

En generell utvecklingstendens är att krisberedskapsområdet påverkats av den förändrade hotbilden som suddar ut gränserna mellan militär och civil beredskap och att distinktionen mellan intern och extern säkerhet blivit allt mindre relevant. Även synen på skyddet av den kritiska infrastrukturen har tagit samma gång då det under kalla kriget främst var angrepp från en extern fiende som stod i fokus men där det nu snarare handlar om att kunna skydda infrastrukturen mot ett mycket bredare spektrum av hot. Jämte denna förändring har samtidigt människors acceptans för exempelvis tele- och elavbrott minskat. Utvecklingen av skyddet av den kritiska infrastrukturen kan också sägas vara ett resultat av att ett flertal kriser såsom terrordåd, elavbrott, naturkatastrofer och pandemier har drivit på det ökade behovet och därmed satsningarna på att skapa gemensamma strukturer och program för att hantera gränsöverskridande kriser.[25]

> Europas medborgare förväntar sig att viktig infrastruktur också fortsättningsvis skall fungera, oberoende av vilken organisation som äger eller driver de enskilda delarna. De förväntar sig att medlemsstaternas myndigheter och EU skall spela en ledande roll för att se till att så sker. De förväntar sig att alla myndighetsnivåer samt ägare och operatörer inom den privata sektorn skall samarbeta för att säkerställa kontinuiteten i de tjänster som Europa är beroende av.[26]

Från en sektorsspecifik till en sektorsövergripande approach
Idag är skydd av kritisk infrastruktur (CIP) en fråga högt uppe på olika nationella och internationella agendor – inte minst inom EU. Inom EU-

[24] Eriksson, Barck-Holst (2005) s.33ff.
[25] Eriksson, Barck-Holst (2005) s.15
[26] KOM(2004) 702 slutlig MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET: ”Skydd av viktig infrastruktur i kampen mot terrorismen”. Bryssel den 20.10.2004

samarbetet har man redan vidtagit ett antal lagstiftningsåtgärder för att införa exempelvis minimistandarder för skydd av kritisk infrastruktur inom ramen för dess olika politikområden. Detta gäller i synnerhet de sektorer som ansvarar för transport, kommunikationer, livsmedel, energi, arbetsmiljö och folkhälsa. I årtionden har exempelvis inspektioner utförts inom ramen för Euratom-fördraget för att kontrollera att radioaktivt material används i enlighet med reglerna och på strålskyddsområdet finns på motsvarande sätt en omfattande lagstiftning som gäller risker med driften av anläggningar och användningen av energikällor som innehåller radioaktiva ämnen.[27] Karaktären på samarbetet varierar dock mellan de olika sakområdena - i vissa fall är samarbetet väldigt långtgående med omfattande regelverk och EU-ledda inspektioner medan det i andra fall snarare handlar om ramlagstiftning som medlemsstaterna själva bestämmer hur man ska genomföra och kontrollera.[28]

Pär Eriksson och Svante Barck-Holst beskriver i ”Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys” att man kan urskilja två bilder av EU:s framtida politik för skydd av kritisk infrastruktur: ”ett kommissionskontrollerat, centraliserat system med en uppifrån-och-ned-process för att identifiera, analysera och skydda kritisk infrastruktur” och ”ett decentraliserat system där EU:s roll är att befrämja en ökad grad av samsyn, koordination och samverkan när det gäller skydd av kritisk infrastruktur men där den konkreta kontrollen över CIP ligger kvar hos medlemsstaterna”. I det första centraliserade systemet betonas alltså gemensamma ramar, kriterier och processer medan det i det decentraliserade systemet mer handlar om utbyte av kunskap och erfarenheter.[29]

Vari består då mervärdet med en sektorsövergripande politik för skydd av kritisk infrastruktur? Mervärdet i att frågan även behandlas sektorsövergripande inom EU brukar förenklat förklaras med att unionen kan stödja kunskapsförmedlingen mellan medlemsstaterna och bygga upp en gemensam kunskaps- och begreppsapparat vilket är en förutsättning för samarbete mellan länderna. En annan effekt är att ett kunskapsutbyte ökar möjligheten att medlemsstaterna uppmärksammar brister i det nationella arbetet med skydd av kritisk infrastruktur som kanske annars hade kunnat passera obemärkt förbi. Slutligen betonas att man genom EU-samarbetet också kan stödja medlemsstater som inte kommit så långt i arbetet vilket i förlängningen även är till nytta för grannländerna.[30]

---

[27] KOM(2004) 702 slutlig MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET: ”Skydd av viktig infrastruktur i kampen mot terrorismen”. Bryssel den 20.10.2004

[28] Eriksson, Barck-Holst (2005) s.39-47. Ser man t.ex. till skydd mot kemolyckor finns där redan ett formaliserat europeiskt inflytande inkl. inspektioner av infrastrukturer medan det på andra områden som t.ex. kontroll av dricksvatten visserligen finns detaljerade EU-direktiv men där det är medlemsländerna som står för implementering och uppföljning. Se vidare Eriksson, Barck-Holst (2005) bilaga 2 för en beskrivning av CIP-arbetet inom några utvalda sakpolitikområden.

[29] Eriksson, Barck-Holst (2005) s.10

[30] Regeringens Fakta-PM 2006/07:FPM67

Som ovanstående genomgång visar kan man sammanfatta att krisberedskapsarbetet inom EU har växt fram sektorsvis inom unionens olika politikområden och att det är först på senare tid som initiativ har tagits för att skapa sektorsövergripande strukturer.[31]

EPCIP:s framväxt kan direkt kopplas till terrordåden i USA den 11:e september 2001, Madridbomberna 2004 samt Londonattentatet 2005 vilka alla bidrog till att man identifierade ett behov av en sektorsövergripande politik för skydd av kritisk infrastruktur.[32] Arbetet med att ta fram ett europeiskt program för skydd av kritisk infrastruktur inleddes formellt i juni 2004 i och med det Europeiska rådets beslut att ett sådant borde inrättas. Kort därefter gavs kommissionen i uppdrag att utarbeta en övergripande strategi för skydd av kritisk infrastruktur och den 20 oktober 2004 antogs följaktligen meddelandet ”Skydd av kritisk infrastruktur i kampen mot terrorismen” med tydliga förslag om vad som skulle kunna förbättra de förebyggande åtgärderna, beredskapen och insatserna.[33] Utarbetandet av EPCIP var därefter föremål för ett intensivt arbete under hela 2005 och kommissionen arrangerade bl.a. två seminarier där man efterlyste idéer och kommentarer från medlemsstaterna.[34] Som en följd av det offentliga samrådet med medlemsstater, näringsliv och experter lade kommissionen i slutet av år 2005 fram en grönbok[35] som angav grunddragen till de olika alternativen för det europeiska programmet för skydd av kritisk infrastruktur. Drygt ett år efter publiceringen av grönboken, den 12 december 2006, lade kommissionen slutligen fram sitt förslag till direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna.[36]

Nästa kapitel (3.2) beskriver de övergripande ramarna i förslaget till ett direktiv om skydd av kritisk infrastruktur med fokus på de delar av förslaget som föreslås bli bindande. Då EU:s medlemsstater fortfarande förhandlar om den slutliga utformningen av direktivet i rådsarbetsgruppen för skydd och beredskap (ProCiv) går det dock inte att i skrivande stund uttala sig om hur programmet i detalj slutligen kommer att utformas. Efter en genomgång av de centrala artiklarna i direktivet ges även en bild av medlemsstaternas övergripande ståndpunkter till direktivet samt utestående frågor inför de fortsatta förhandlingarna.

---

[31] Eriksson, Barck-Holst (2005) s.7

[32] Även om terrorismbekämpningen har fungerat som en slags katalysator för EU:s samlade arbete med krishanteringsfrågor (inklusive CIP) baseras EPCIP på en helhetssyn på hot och risker och omfattar således alla relevanta risker (en s.k. all-hazards approach).

[33] KOM(2004) 702 slutlig MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET: ”Skydd av viktig infrastruktur i kampen mot terrorismen”. Bryssel den 20.10.2004

[34] Det första seminariet om skydd av EU:s kritiska infrastruktur hölls den 6–7 juni 2005 och det andra EU-seminariet hölls den 12–13 september 2005. Såväl medlemsstater som näringslivsorganisationer deltog i detta seminarium. Kommissionen har också genomfört s.k. expertseminarier för att inhämta berörda aktörers synpunkter. KBM, Vägverket, Post- och telestyrelsen samt Energimyndigheten deltog från svensk sida på dessa expertseminarier.

[35] Den 17 november 2005 antog kommissionen grönboken om ett europeiskt program för skydd av kritisk infrastruktur. En grönbok är i EU-terminologin ett ”paper” 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. (KOM (2005) 576 slutlig)

[36] Meddelande från Kommission om ett europeiskt program för kritisk infrastruktur, Bryssel den 12.12.2006 KOMMISSIONEN (2006) 786 slutlig.

3.2 Det europeiska programmet för skydd av kritisk infrastruktur

Lite förenklat kan man säga att EPCIP är ett sektorsövergripande handlingsprogram som syftar till att specificera de åtgärder som ska vidtas för att skydda europeisk kritisk infrastruktur. Målet med inrättandet av ett europeiskt program för skydd av viktig infrastruktur är framförallt att säkerställa lika nivåer avseende skyddsåtgärderna för den viktiga infrastrukturen, ett minimalt antal svaga punkter samt snabba och testade återhämtningsåtgärder inom unionen.

Det europeiska programmet för skydd av kritisk infrastruktur föreslås bestå av tre huvuddelar; (1) ett direktiv, (2) ett finansieringsprogram[37] och (3) ett förslag till informations- och varningssystem (CIWIN).[38] Då själva förfarandet för att fastställa och klassificera europeisk kritisk infrastruktur och etablerandet av en gemensam strategi för bedömning av behoven av att stärka denna kommer att regleras i ett direktiv kommer endast direktivet att behandlas i denna framställning.

Vid genomförandet av EPCIP har man fastslagit ett antal huvudprinciper som ska vara ledande i arbetet. Kommissionens insatser ska bl.a. med beaktande av subsidiaritetsprincipen inriktas på kritisk infrastruktur ur ett europeiskt snarare än ett nationellt eller regionalt perspektiv. Kommissionen ska vidare undvika överlappningar med insatser som redan görs på EU-nivå, nationellt eller regionalt när dessa har visat sig effektiva för att skydda kritisk infrastruktur och således bara utgöra ett komplement. Utbytet av information om kritisk infrastruktur ska ske med beaktande av lämplig sekretess i en atmosfär av tillit och säkerhet. Vidare ska alla berörda aktörer involveras i utvecklingen och genomförandet av EPCIP och åtgärderna ska vara proportionella i förhållande till risknivån och typen av hot. Eftersom olika sektorer har sina särskilda erfarenheter, sakkunskaper och krav när det gäller skyddet av kritisk infrastruktur, kommer EPCIP att utvecklas på sektorsbasis och genomföras i enlighet med en förteckning över sektorer med kritisk infrastruktur som berörda aktörer har enats om.[39]

Lite förenklat kan man dela in det europeiska programmet för skydd av kritisk infrastruktur i icke-bindande och bindande åtgärder. Bland de icke-bindande åtgärderna ingår bl.a. att delta i expertgrupperna för skydd av

[37] I syfte att stödja utvecklingen av EPCIP antog rådet i februari 2007 ett finansieringsprogram för ”Förebyggande, beredskap och konsekvenshantering när det gäller terrorism och andra säkerhetsrelaterade risker”. Programmet ryms inom ramen för det större programmet ”Säkerhet och skydd av friheter” och har en total budget på 140 miljoner euro för sjuårsperioden 2007–2013. Finansieringsprogrammet kan bland annat stödja metodutveckling, operativa åtgärder, utveckling av säkerhetsstandarder samt samordning och samarbete inom EU när det gäller kritisk infrastruktur. När det gäller konsekvenshantering kan programmet finansiera utbyte av kunskap och erfarenheter för att fastställa best practices samt gemensamma övningar och scenarier.

[38] Critical Infrastructure Warning Information Network, CIWIN. Ett nätverk för varningar om hot mot kritisk infrastruktur föreslås inrättas genom ett separat kommissionsförslag. Nätverket föreslås användas för utbyte av god praxis. Läs mer om CIWIN i Kjellén (2007) “Redovisning av EU:s varningssystem” s. 36

[39] Mötesanteckningar från ProCiv [12 december 2007]

infrastruktur på EU-nivå; att tillämpa en process för utbyte av information om skydd av kritisk infrastruktur; att kartlägga och analysera beroendeförhållanden; att utarbeta nationella program för skydd av kritisk infrastruktur samt att kartlägga nationell kritisk infrastruktur. Bland de bindande åtgärderna i det nuvarande direktivförslaget ingår i sin tur att kartlägga och definiera europeisk kritisk infrastruktur; att genomföra hot- och riskbedömningar avseende europeisk kritisk infrastruktur; att utarbeta säkerhetsplaner och utse sambandsansvariga för säkerhetsfrågor samt att utse kontaktpunkter för skydd av europeisk kritisk infrastruktur.

Totalt innehåller direktivförslaget 14 artiklar. Det centrala innehållet utgörs bland annat av definitionerna i artikel 2, riktlinjerna för identifieringen av europeisk kritisk infrastruktur i artikel 3, klassificeringen av europeisk kritisk infrastruktur i artikel 4, inrättandet av säkerhetsplanerna i artikel 5, utpekandet av sambandsansvariga i säkerhetsfrågor i artikel 6 och de nationella hot- och riskbedömningarna i artikel 7. Dessutom utgör skrivningarna om sekretess i artikel 9 och kontaktpunkterna för CIP-frågor (artikel 10) viktiga förutsättningar för verksamheten.[40]

I *artikel 1* presenteras direktivets syfte vilket är att fastställa ett gemensamt förfarande för att kartlägga och klassificera europeisk kritisk infrastruktur. Syftet med direktivet är även att föreskriva om bedömningen av behovet av ett stärkt skydd.

I *artikel 2* redogörs för de termer som är viktigast i förhållande till direktivet och programmet. I artikeln definieras bl.a. termer som ’kritisk infrastruktur’; ’europeisk kritisk infrastruktur (ECI)’; ’riskanalyser’; ’känslig CIP-relaterad information’; ’prioriterade sektorer’; ’skydd’ samt vad som åsyftas med ’ägare och operatörer av ECI’. Kommissionen föreslår att definitionen av europeisk kritisk infrastruktur (ECI), vilket utgör basen för arbetet, ska vara ”kritisk infrastruktur som vid driftsstörning eller förstörelse skulle få betydande följder för två eller fler medlemsstater, eller en enskild medlemsstat om den kritiska infrastrukturen finns i en annan medlemsstat”.

I *artikel 3* regleras hur europeisk kritisk infrastruktur ska kartläggas. Förfarandet är indelat i tre steg. I det första steget fastställer kommissionen i samarbete med medlemsstaterna och de parter som berörs, såväl tvärsektoriella och sektorsspecifika kriterier som antas formellt genom ett kommittéförfarande. Kriterierna fastställs bl.a. med hänsyn till hur allvarliga de ekonomiska, miljömässiga och publika effekterna blir om ett objekt skadas. Direktivet stipulerar att ett omfattande identifieringsarbete av potentiella ECI inom och utanför en medlemsstats gränser ska vara genomfört av varje land senast 12 månader efter att ett beslut om direktiv fattats. Identifieringsarbetet ska vara en kontinuerlig process.[41]

---

[40] Förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna. Samtliga artiklar i nedanstående presentation är återgivna från den i dagsläget senaste versionen som är daterad 19 februari 2008. 5051/2/08 REV 2.

[41] Artikel 3.3. Direktiv 5051/2/08 REV 2 av den 19 februari 2008. I tidigare utkast föreslogs att identifieringsarbetet skulle vara genomfört 6 månader efter att ett beslut om direktiv fattats.

I *artikel 4* regleras hur europeisk kritisk infrastruktur ska utpekas. Inom 15 månader efter att tvärsektoriella och sektorsspecifika kriterier har antagits ska alla medlemsländer ha informerat andra berörda medlemsstater som kan påverkas samt ha redogjort för skälen till att utpeka det som europeisk kritisk infrastruktur.[42] Varje medlemsstat som har en ECI på sitt territorium ska därefter inleda bilaterala och/eller multilaterala diskussioner med berörda medlemsstater. Kommissionen kan delta i dessa diskussioner men kommer inte att ha tillgång till detaljerad information. Medlemsstaten som har en ECI på sitt territorium måste lämna sitt godkännande för att en ECI ska kunna pekas ut.[43] Inom 24 månader, och därefter på årlig basis, ska kommissionen informeras sektorsvis kring arbetsläget samt antalet medlemsstater som är beroende av den europeiskt kritiska infrastrukturen. Endast de medlemsstater som berörs av en ECI ska veta dess identitet.[44]

I *artikel 5* behandlas inrättandet av säkerhetsplaner, Operator Security Plans (OSP). Denna artikel ålägger ägarna eller operatörerna av utpekad europeisk kritisk infrastruktur en skyldighet att inom ett år efter utpekandet av en ECI upprätta en säkerhetsplan i enlighet med direktivets bilaga II.[45] Säkerhetsplanen ska bl.a. innehålla vilka anläggningar som är kritiska, en riskanalys som bygger på hotscenarier och effekter av dessa samt vad som görs för att skydda den kritiska infrastrukturen, både permanent och vid en kris.[46] Medlemsstaternas myndigheter ska därefter, med hjälp av säkerhetsplanerna, utöva tillsyn över dessa anläggningar. Medlemsstaterna ska sedan på ett övergripande plan rapportera sårbarheter, risker och hot till kommissionen per sektor (genom en utpekad CIP-Contact Point). I de fall tillfredsställande säkerhetsarrangemang redan existerar berörs ej dessa av denna artikel.

I *artikel 6* föreskrivs att varje medlemsstat genom lagar eller andra regleringar ska garantera att sambandsansvariga i säkerhetsfrågor, Security Liaison Officers (SLO) finns utpekade för alla objekt som klassificerats som europeisk kritisk infrastruktur. Tanken är att personen som utpekas som SLO ska agera som kontaktpunkt i säkerhetsfrågor gentemot den relevanta myndigheten i medlemsstaten.

> If a member state satisfies itself that a designated European Critical Infrastructure does not have a Security Liaison Officer, it shall ensure that either by laws or regulations or by

[42] Artikel 4.1. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[43] Artikel 4.3. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[44] Artikel 4.4. Direktiv 5051/2/08 REV 2 av den 19 februari 2008. I tidigare förslag till direktiv fanns en artikel om upprättande av listor av europeisk kritisk infrastruktur som skulle förvaras i kommissionens regi. Flera medlemsstater var emellertid kritiska till detta eftersom upprättandet av sådana listor skulle kunna riskera att motverka det EPCIP skapades för att skydda om informationen skulle hamna i ”fel” händer. Detta resulterade i att skrivningen sedermera exkluderades ur direktivförslaget.
[45] Kommissionen har understrukit att annexen ska beslutas samtidigt som beslut tas om direktivet i sin helhet med reservation för att man bara kommer hinna ta fram sektoriella kriterier för de prioriterade sektorerna, dvs. transporter, energi samt eventuellt informations- och kommunikationsteknologier.
[46] En lista på redan antagna åtgärder, principer och riktlinjer inom olika sektorer som kan sägas tillfredställa de krav som direktivförslaget lägger vad gäller Operator Security Plans återges i annex fyra i direktivförslaget. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.

> measures, principles or guidelines the owners/operators of designated ECI located on its territory designate a Security Liaison Officer. The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the European Critical Infrastructure and the relevant Member State authority.[47]

För såväl upprättandet av OSP som inrättandet av SLO gäller att om sektorn redan uppfyller de krav som föreskrivs i direktivet behöver man endast hänvisa till befintliga regler.[48]

Artikel 6.2 stipulerar vidare att varje medlemsstat ska inrätta en lämplig kommunikationsmekanism mellan den relevanta myndigheten och den som är utpekad som sambandsansvarig i säkerhetsfrågor i syfte att utbyta relevant information gällande identifierade hot och risker i förhållande till den utpekade europeiskt kritiska infrastrukturen.[49]

I *artikel 7* föreskrivs om rapportering. Inom 12 månader efter det att en ECI utpekats ska varje medlemsstat genomföra en riskanalys kring denna för att därefter var 24:e månad ge en generell sektorsvis lägesbeskrivning till kommissionen. Gemensamma riktlinjer för hur man ska genomföra riskanalyser i förhållande till en ECI kan komma att utvecklas på en sektoriell basis men antagande av sådana riktlinjer kommer att vara frivilliga för medlemsstaterna. Även en gemensam mall för rapporterna som lämnas in till kommissionen kommer att tas fram. Enligt nu liggande förslag gäller att om man bara har en ECI inom en sektor rapporterar man om den, inte om de andra sektorerna.[50] Baserat på dessa rapporter kan kommissionen och medlemsstaterna besluta om möjliga åtgärder som måste vidtas, t.ex. vad gäller övning, utbildning, erfarenhetsutbyte etc. Kommissionen har dock meddelat att de säkerhetshöjande åtgärder som kan komma att krävas inte kommer att kunna bekostas av EU:s gemensamma budget. Detta innebär att sådana kostnader, om det finnes nödvändigt, till övervägande del kommer att bäras av privata ägare och förvaltare av europeiskt kritisk infrastruktur.[51]

I *artikel 8* ges kommissionen möjlighet att, genom relevanta medlemsstatsorgan, stödja ägarna/operatörerna av en europeisk kritisk infrastruktur genom att bidra med tillgång till best practices. I de fall det behövs särskild sakkunskap kan kommissionen exempelvis inrätta expertgrupper på EU-nivå för skydd av kritisk infrastruktur. Expertgrupperna ska stödja EPCIP genom att underlätta utbytet av synpunkter i frågor som rör skydd av kritisk infrastruktur och fylla en

[47] Artikel 6.1. Direktiv 5051/2/08 REV 2 av den 19 februari 2008. Tidigare var kraven på OSP och SLO mycket hårdare men efter att flera medlemsstater uttryckt en önskan om att se en mer frivillig approach gällande såväl OSP som SLO har kommissionen presenterat nya skrivningar på området. KOM 14915/2/07 REV 2 [23 november 2007].
[48] Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[49] Artikel 6.2. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[50] Artikel 7. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[51] Dock finns en möjlighet att erhålla finansiella medel från kommissionens program ”Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks” som sträcker sig över perioden 2007–2013 för att öka skyddet av kritisk infrastruktur genom exempelvis satsningar på övning, utbildning och forskning.

rådgivande funktion. Expertgruppernas funktioner kan dock variera mellan olika sektorer för skydd av infrastruktur, med hänsyn till vad som är karakteristiskt för den enskilda sektorn.[52] Expertgrupperna kommer inte att ersätta andra grupper som redan har inrättats eller som skulle kunna anpassas så att de uppfyller behoven i samband med EPCIP.

Då verksamheten förutsätter särskild försiktighet berör *artikel 9* hanteringen av konfidentiella uppgifter, sekretess och utbyte av information (även muntlig) i fråga om skyddet av den kritiska infrastrukturen.

I *artikel 10* föreskrivs om nationella kontaktpunkter. Här föreslås att varje medlemsstat bör utse en kontaktpunkt, en s.k. CIP-Contact Point, som samordnar frågor som rör skydd av europeisk kritisk infrastruktur inom den egna medlemsstaten samt gentemot andra medlemsstater och kommissionen.[53]

Artikel 11 i direktivet anger att kommissionen ska assisteras av en kommitté bestående av medlemsstatsrepresentanter där artikel 5 och 7 i beslut 1999/468/EC ska gälla. Med s.k. kommittologiförfarande menas att kommissionen måste samråda med särskilda kommittéer när den genomför EU-lagstiftning. Syftet med kommittéförfarandet är att kommissionen genom kommittologiförfarandet kan föra en dialog med förvaltningen i medlemsländerna innan den vidtar genomförandeåtgärder och därmed också se till att åtgärderna på bästa möjliga sätt motsvarar verkligheten i vart och ett av de berörda länderna. Kommittéerna består av experter från EU-länderna och en representant för kommissionen som ordförande, vilket innebär att det är kommissionen som sammankallar kommittéerna och sätter dagordningen.[54]

Artikel 12 reglerar genomförande och implementering och fastslår att EU:s medlemsstater senast två år efter direktivets ikraftträdande ska vidta

[52] Funktionerna kan bl.a. handla om att bistå med att definiera sårbarheter, ömsesidiga beroenden och bästa praxis inom en sektor. En annan funktion kan vara att bistå vid utarbetandet av åtgärder för att minska och/eller undanröja allvarliga sårbarheter, bistå vid utvecklingen av resultatindikatorer eller att underlätta informationsutbyte, fortbildning och uppbyggnad av ömsesidigt förtroende på området. Expertgrupperna kan också utveckla och framhålla ”konkreta typfall” för att till andra verksamheter inom sektorn förmedla värdet av att medverka i planer och initiativ när det gäller skydd av infrastruktur eller tillhandahålla sektorsspecifika sakkunskaper och råd om olika ämnen (till exempel forskning och utveckling).

[53] Artikel 10. Direktiv 5051/2/08 REV 2 av den 19 februari 2008. Att man utser en kontaktpunkt för skydd av kritisk infrastruktur hindrar inte att andra myndigheter i en medlemsstat deltar i behandlingen av frågor om skydd av europeisk kritisk infrastruktur.

[54] Det finns olika typer av kommittéer som i sin tur har olika möjlighet att utöva inflytande över kommissionens beslut; rådgivande kommittéer avger yttranden som kommissionen ska ta hänsyn till. Detta förfarande används i allmänhet när de ärenden som behandlas inte är politiskt känsliga då denna typ av kommitté ger medlemsländerna minst inflytande över kommissionen. Om man använder sig av förvaltningskommittéer och de åtgärder som kommissionen antar inte är förenliga med kommitténs yttrande ska kommissionen överlämna dem till rådet, som får fatta ett annat beslut. Här krävs dock kvalificerad majoritet i både kommitté och ministerråd för att förkasta kommissionens förslag. Om en föreskrivandekommitté (regulatory committée) tillsätts får kommissionen endast anta genomförandeåtgärder om medlemsländerna i kommittén ställer sig positiva till dessa. I dessa kommittéer har medlemsländerna m a o störst möjlighet att blockera ett förslag från kommissionen. Det aktuella direktivet kommer att genomföras med hjälp av en föreskrivande kommitté. Källa: EU-upplysningen.

nödvändiga åtgärder för att uppfylla förpliktelserna som följer av direktivet. Därefter ska varje medlemsstat informera kommissionen om detta samt uppvisa skrivningarna om de åtgärder som vidtagits och deras överensstämmelse med direktivet.[55]

Artikel 13 och *artikel 14* reglerar slutligen ikraftträdandet och stipulerar att direktivet ska träda ikraft på den 20:e dagen efter publiceringen i the Official Journal of the European union och rikta sig till alla medlemsstater.

I direktivets *bilaga I* finns en förteckning över sektorer där infrastrukturer förväntas förekomma. Av förteckningen framgår att man i dagsläget har identifierat 11 sektorer: (1) energi, (2) kärnindustri, (3) informations- och kommunikationsteknik, (4) vatten, (5) livsmedel, (6) hälso- och sjukvård, (7) finans, (8) transporter, (9) kemisk industri, (10) rymdforskning och (11) forskningsanläggningar. *Bilaga II* i direktivet ger en övergripande beskrivning av vad som ska ingå i de säkerhetsplaner som direktivet stipulerar ska finnas över varje utpekad ECI. *Bilaga III* fastställer proceduren för identifikationen av ECI enligt direktivets artikel 3.3. *Bilaga IV* kopplat till direktivet innehåller slutligen en icke uttömmande lista över åtgärder, principer och riktlinjer tillämpbara på vissa sektorer och som bedöms uppfylla kravet på upprättandet av Operator Security Plans.[56]

3.3 EPCIP:s nuvarande status och utestående frågor

En granskning av kommissionens sammanställning av medlemsstaternas synpunkter[57] på grönboken 2005 ger vid handen att samtliga medlemsstater välkomnade initiativet och arbetet med utvecklandet av ett europeiskt program för skydd av kritisk infrastruktur. Flera medlemsstater framhöll dock subsidiaritetsprincipen som särskilt viktig att ta i beaktande i sammanhanget. Av de granskade länderna inom ramen för denna studie framhöll bl.a. Storbritannien, Danmark och Nederländerna att medlemsstaterna fortfarande bör inneha ansvaret för att garantera säkerheten för den kritiska infrastrukturen och uppgav vid grönbokskonsultationerna att de motsatte sig någon form av legal ram. Flera medlemsstater hänvisade också till olika legala traditioner och organisationssystem i medlemsstaterna och underströk vikten av att EPCIP tar hänsyn till detta. Gällande EPCIP:s omfattning framhöll Sverige och Finland att EPCIP bör ha en bred syn på hot och risker dvs. en s.k. all-hazard approach. De övriga tre undersökta medlemsstaterna gav också sitt stöd för en all-hazard approach men ansåg att denna trots allt skulle fokusera på terrorism. På frågan om ett EPCIP-ramverk skulle vara obligatorisk eller frivillig uppgav Sverige, Danmark och Storbritannien att de förespråkade en frivillig approach medan Nederländerna framhöll att ramverket först bör vara frivilligt för att därefter bli obligatoriskt när det är testat och väl etablerat. Finland avgav ingen tydlig åsikt i frågan.[58]

[55] Artikel 12. Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[56] Direktiv 5051/2/08 REV 2 av den 19 februari 2008.
[57] Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006. Sammanlagt inkom officiella svar från 22 medlemsstater. Italien, Grekland och Malta svarade inte.
[58] Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006.

Alla fyra länder inom ramen för denna studie argumenterade för att kriterierna för att identifiera europeisk kritisk infrastruktur skulle utarbetas sektorsvis. Av de undersökta medlemsstaterna var det dock endast Finland som uttryckte sitt stöd för att definitionen av europeisk kritisk infrastruktur skulle utgå ifrån infrastruktur som kan få gränsöverskridande effekter för två eller fler medlemsstater. De övriga länderna som granskats inom ramen för denna studie (Danmark, Nederländerna och Storbritannien) förespråkade att definitionen skulle utgå ifrån infrastrukturhaveri som drabbar tre eller fler medlemsstater.[59] En majoritet av samtliga medlemsstater underströk att medlemsstatens godkännande ska krävas för att en ECI ska kunna utpekas på ett lands territorium. Många av medlemsstaterna framhöll i sammanhanget att om EPCIP förbereds och genomförs korrekt skulle situationer där det föreligger meningsskiljaktigheter kring ECI-status eller ej vara väldigt ovanliga. Inom ramen för EPCIP föreslogs vidare utvecklandet av en gemensam metod för att identifiera och klassificera olika typer av hot, risker och sårbarheter. Samtliga av de undersökta länderna, undantaget Finland, motsatte sig detta.

I grönboken restes också frågan om den nationella kritiska infrastrukturens roll inom EPCIP. Danmark, Nederländerna och Storbritannien motsatte sig detta och deklarerade att nationell kritisk infrastruktur bör ligga utanför ramen för EPCIP. Finland och Sverige framhöll att det bästa vore om delar av EPCIP på frivilligbasis skulle kunna användas i relation till nationell kritisk infrastruktur men att det inte skulle vara något obligatorium på detta. Gällande inrättandet av en CIP Contact Point uttryckte Finland sitt stöd för en single coordinating body medan de övriga länderna i studien förespråkade en kontaktpunkt som det var upp till varje enskild medlemsstat att organisera. Kring upprättandet av säkerhetsplaner framhöll Danmark, Nederländerna och Storbritannien att OSP-konceptet skulle användas som best practice för de ägare och operatörer som har liten erfarenhet av att hantera liknande frågor.[60]

Vad gäller inrättandet av ett varnings- och informationssystem (CIWIN) uttryckte Finland sitt stöd för detta medan Danmark, Nederländerna och Sverige förespråkade att begränsa CIWIN till ett forum för utbyte av idéer och best practice kopplat till skydd av kritisk infrastruktur. Storbritannien motsatte sig inrättandet av ett varnings- och informationssystem i någon som helst form och framhöll att CIWIN som kommunikationskanal inte skulle tillföra något utöver det som redan existerar.[61]

Vid det sista ProCiv-mötet år 2007 framgick att medlemsstaterna fortfarande är oeniga på ett antal punkter i direktivet. Utestående frågor är bl.a. vilken status rättsinstrumentet ska ha (direktiv eller rådsbeslut), hur ECI ska definieras, samt hur kriterium för ECI ska skapas (det sistnämnda

[59] Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006.
[60] Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006.
[61] Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006.

har avgörande betydelse för hur många ECI varje land kommer att ha inom sina gränser).[62]

Lite förenklat kan man säga att ett direktiv är en rättsakt som är riktad till medlemsländerna och som är bindande vad gäller de mål som ska uppnås och när det ska ske. Länderna beslutar dock fortfarande själva vad som ska göras för att föreskrifterna i direktivet ska uppfyllas, men vid tvist är det EG-domstolen som avgör om så skett. Länderna som förespråkar ett rådsbeslut argumenterar å sin sida för att ett rådsbeslut inte skulle innebära samma hårda styrning från EU:s sida som ett direktiv vilket skulle ge medlemsländerna ett större och friare ansvar att utforma sin egen verksamhet. Rent teoretiskt skulle den gemensamma ramen för EPCIP kunna vara frivillig eller obligatorisk – eller en blandning av båda. Båda typerna av ramverk skulle kunna komplettera redan existerande sektoriella och horisontella åtgärder på EG- och medlemsstatsnivå. Kommissionen argumenterar dock för att det endast är en lagstiftningsram som kan ge en rättslig grund för ett konsekvent och enhetligt genomförande av åtgärder till skydd för europeisk kritisk infrastruktur och att icke bindande frivilliga åtgärder inte skulle ge någon klarhet i vem som ska göra vad samtidigt som det är osäkert hur ett icke-bindande beslut skulle tas emot i de olika medlemsstaterna. Ett försök till sammanfattning av samtliga medlemsstaters ståndpunkter i frågan ger vid handen att Frankrike, Slovakien, Ungern, Spanien och Rumänien ger ett klart stöd till en fortsatt process till förmån för ett direktiv. Slovenien, Lettland, Spanien, Italien, Storbritannien, Nederländerna, Finland, Bulgarien och Malta stödjer också en sådan process men är öppen för en kompromisslösning medan Tjeckien, Danmark, Sverige och Tyskland argumenterar för det tyska förslaget om ett icke-tvingande rådsbeslut för informationsdelning.[63]

Frågan kring hur man ska definiera europeisk kritisk infrastruktur rör sig något förenklat kring hur många stater en kritisk infrastruktur ska omfatta för att bli utpekad som europeisk kritisk infrastruktur. Här föreslår kommissionen att definitionen av europeisk kritisk infrastruktur, vilket utgör basen för arbetet, ska vara ”kritisk infrastruktur som vid driftsstörning eller förstörelse skulle få betydande följder för två eller fler medlemsstater, eller en enskild medlemsstat om den kritiska infrastrukturen finns i en annan medlemsstat” medan länder som Storbritannien, Nederländerna, Sverige, Tyskland, Danmark m.fl. önskar att en kritisk infrastruktur ska beröra tre eller fler stater för att definieras som europeisk kritisk infrastruktur.[64]

Vid rådet för inrikes- och rättsliga frågor i december 2007 presenterade det portugisiska ordförandeskapet resultaten av förhandlingarna och dess nuvarande status i en s.k. Progress Report och Slovenien har meddelat att

[62] Artikel 3 i direktivförslaget behandlar identifiering av europeisk kritisk infrastruktur (ECI). Kommissionen har hittills bara lämnat förslag på tvärsektoriella kriterier för utpekande av ECI. Dessa presenterades vid PrcCiv-mötet den 30 oktober. Diskussioner har också påbörjas inom ramen för den s.k. CIP Contact Group den 21 november 2007.

[63] Under höstens förhandlingsomgång lade bl.a. Tyskland fram ett förslag på ett icke-tvingande rådsbeslut för informationsdelning som initialt mottogs positivt bland många länder men som nu kommit alltmer i skymundan. Mötesanteckningar från ProCiv, [12 december 2007]

[64] Mötesanteckningar från ProCiv, [12 december 2007]

direktivsförhandlingarna kommer att fortgå även under deras ordförandeskap våren 2008.[65]

[65] Mötesanteckningar från ProCiv, [12 december 2007]

4 DANMARK

I nedan sektion ges en översiktlig beskrivning av Danmarks krishanteringssystem med fokus på vad man definierar som kritisk infrastruktur, hur ansvars- och ledningsstrukturer ser ut, vilken roll de lokala myndigheterna, departementen och andra centrala aktörer har och hur CIP-åtgärder finansieras. Avsnittet avslutas med en sammanfattning av den danska synen på EPCIP och vilka förberedelser som har vidtagits.

Förkortningar

BRS	Beredskabsstyrelsen
FE	Forsvarets Efterretningstjeneste
PET	Politiets Efterretningstjeneste

4.1 Landets arbete med skydd av kritisk infrastruktur

Till skillnad från många andra länder var krisberedskap en perifer fråga i Danmark även efter terrorattentaten i USA den 11 september 2001. Traditionellt har man i Danmark arbetat så att man vart fjärde år utvecklar en överenskommelse, ett politiskt s.k. aftale, för varje område och detta gällde i princip också krisberedskapen som avhandlades en gång vart fjärde år och sedan hade Beredskabsstyrelsen (BRS)[66] inte särskilt mycket kontakter med den politiska nivån förrän det var dags att diskutera nästa fyraårsperiod. Efter att den danske statsministern Anders Fogh Rasmussen meddelade att man skulle slå ihop militärt och civilt försvar har det dock skett många förändringar i den danska krisberedskapen och för första gången finns nu en samlad politik för dansk krisberedskap.[67]

I juni 2005 offentliggjorde regeringen sin överordnade politik för beredskapsområdet med titeln: ”Et robust og sikkert samfund - regeringens politik for beredskabet i Danmark”.[68] Här fastlade regeringen de överordnade riktlinjerna för det fortsatta arbetet med att förebygga större olyckor och katastrofer samt hantera större händelser och konsekvenserna härav. Regeringen prioriterade följande åtta områden: (1) koordinering, (2) förebyggande, (3) beredskapsplanering, (4) insatsberedskap, (5) utbildning och övningar, (6) utvärdering, analyser och kunskapsuppbyggnad, (7) internationell utveckling och samarbete samt (8) CBRN-beredskap.[69]

[66] BRS ansvarar likt KBM för att samordna samhällets krisberedskap, att säkerställa att utvecklingen sker samordnat och att samhällets resurser används så effektivt som möjligt. BRS har dock ett bredare uppdrag än KBM och arbetar även med frågor som rör exempelvis kärnkraftberedskap, operativt räddningsarbete och internationella insatser i katastrofområden. International CEP Handbook (2006) Danmark s. 57-60

[67] Mötesanteckningar från det nordiska GD-mötet den 28 september 2005 s. 5 (ej publicerad)

[68] Et robust og sikkert samfund – Regeringens politik for beredskabet i Danmark (2005)

[69] Et robust og sikkert samfund – Regeringens politik for beredskabet i Danmark (2005). CBRN är en förkortning för kemiska, biologiska, radiologiska och nukleära hot och risker.

Den danska strukturen för krisberedskap består av sektorerna räddningsberedskap (motsvarar vår räddningstjänst) och den civila sektorns beredskap (motsvarar vårt krishanteringssystem). Båda sektorerna ingår i totalförsvaret. Beredskapen i den civila sektorn i Danmark kan överordnat delas in i två delar; ”insatsberedskap” som har till uppgift att hantera omedelbara konsekvenser som berör personer, egendom och miljö i händelse av olyckor mm. samt ”infrastrukturberedskap” som ska säkra att samhällets funktioner kan upprätthållas vid händelse av olyckor mm.[70] Formellt sett ingår polisen och räddningstjänsten i den civila sektorns beredskap men denna påtar ingen överordnad roll i förhållande till dessa sektorer.

I Danmark ligger ansvaret för samhällets beredskap hos respektive myndighet (s.k. sektorsansvar). Enligt beredskabslagen § 24, stycke 1, ska de enskilda ministrarna inom respektive område planera för att upprätthålla samhällets funktioner i händelse av olyckor och katastrofer (inklusive krigshandlingar) samt för att kunna lämna stöd till försvaret. Respektive ministerium ansvarar således också för att det finns planer på hur man upprätthåller samhällets kritiska funktioner inom deras respektive område.[71] I Danmark definieras kritisk infrastruktur som;

> [Kritisk infrastruktur] kan forstås som de elementer i et overordnet system (samfund), der er så vitale, at forstyrrelse og nedbrud af bare en enkelt af dem ville kunne true selve systemets funktionsduelighed.[72]

Den civila sektorns skyldigheter inom beredskapsplaneringen framgår av Beredskapslagens femte kapitel (§§ 24–28). Beredskapslagen stipulerar att den civila sektorn är förpliktigad att planera för hur samhällets kritiska funktioner kan fortsätta att fungera eller snabbt återupprättas vid en olycka eller katastrof. Beredskapen gäller i alla former av krissituationer i freds- och krigstid, naturstyrda som människostyrda och såväl teknologiska hot som terrorhandlingar. I den nationella sårbarhetsutredningen finns en översikt över vilken bredd och struktur på allvarliga händelser som beredskapen ska kunna hantera. Speciellt fokus riktas mot energi-, tele-, IT och transportområdet då de flesta övriga sektorer är beroende av dessa.[73] Beredskapsarbetet omfattar också skydd av kritisk infrastruktur i strikt bemärkelse som exempelvis säkring av anläggningar, installationer och resurser som klassas som samhällets kritiska infrastruktur. I oktober 2005 utgav Beredskabsstyrelsen en vägledning till de centrala myndigheterna om

---

[70] Dessa är naturligtvis nära sammanlänkade och infrastrukturberedskapen har i många fall även en insatskapacitet. Beredskabsstyrelsen, (BRS) ”Helhedsorienteret beredskabsplanlaegning, information, inspiration og praktik” [oktober 2005]

[71] Danmark genomför varje år en nationell sårbarhetsanalys som de myndighetsvisa krishanteringsplanerna är tänkta att komplettera. KBM:s landunderlag: Bilaga A Danmarks krishanteringssystem (ej publicerad)

[72] National Sårbarhedsudredning, Udvalget for National Sårbarhedsudredning. Beredskabsstyrelsen 2004.

[73] Tidigare var beredskap primärt riktat mot krigs- och krigsliknande förhållanden men detta ändrades i och med att det nya beredskapsbegreppet infördes i samband med ändringen av beredskabslagen den 1 juli 2003. Fakta blad, “Den civile sectors beredskab” samt Regeringens redegorelse om beredskabet, Maj 2007. [2007-11-15].

beredskabsplanering: ”Helhedsorienteret beredskapsplanläggning, information, inspiration og praktik”.[74]

Den 1 juli 2003 ändrades begreppet ”det civila beredskab” mot beteckningen ”den civila sektors beredskab” och Beredskapsstyrelsen (BRS) fick då, förutom rollen att koordinera den nationella räddningsberedskapen som man redan innehade, också uppgiften att koordinera planeringen av den civila sektorns beredskap (lag nr. 293). Vid terrorattentat eller andra stora kriser är Beredskabsstyrelsen bemannad dygnet runt och står i kontinuerlig kontakt med polisen och försvaret samt andra myndigheter efter behov.[75]

Då samhället idag är så komplext finns ett stort behov av koordination mellan offentliga och privata verksamheter och institutioner. Å försvarsministeriets vägnar koordinerar BRS beredskapsplaneringen mellan respektive område/ministerium. Försvarsdepartementet har emellertid inte rätt att ta del av andra departements planläggning och kan inte påverka deras krisberedskapsarbete. Till Försvarsdepartementets uppgift hör också att koordinera utnyttjandet av samhällets beredskapsresurser och stärka samspelet mellan de civila och de militära resurserna. Försvarsdepartementet har dock inte några operativa uppgifter vid en kris.[76]

För att tillförsäkra samordning av beredskapsplaneringen - både i nationella och internationella frågor – har sex s.k. faglige koordinationsfora bestående av sektorer med stora ömsesidiga beroenden inrättats.[77] De faglige koordinationsfora, vars fokus främst är planering och inte operativt ansvar, har till uppgift att skapa ett ramverk för ett löpande informations-, kunskaps- och erfarenhetsutbyte på säkerhets och beredskapsområdet i relation till såväl nationella som internationella aktiviteter. Utgångspunkten för deltagandet i ett koordinationsforum är att myndigheterna deltar med sin sektorsspecifika kunskap och bibehåller samma ansvars- och beslutsförhållanden som myndigheten har på alla andra områden.[78]

På senare tid har ett antal nya krisledningsorgan skapats i Danmark. I statsministeriets regi finns bl.a. regeringens sikkerhedsudvalg (ung. ”säkerhetsutskottet”) med ett antal fasta medlemmar bestående av bl.a. statsministern, utrikesministern, försvarsministern och justitieministern samt möjlighet att ta in fler medlemmar efter behov. Det är sikkerhedsudvalget som definierar och fastställer de nationella

[74] Regeringens redegorelse om beredskabet, maj 2007. Beredskabsstyrelsen har utvecklat en modell för risk- och sårbarhetsanalyser (ROS-modellen). Denna är dock inte tänkt att ersätta mer specialiserade analysredskap utan syftar till att komplettera redan existerande metoder.
[75] International CEP Handbook (2006) Danmark s. 57-60
[76] KBM:s landunderlag: Bilaga A Danmarks krishanteringssystem (ej publicerad)
[77] Dessa fora motsvarar på många sätt de svenska samverkansområdena och är (1) Energi, IT och tele, (2) transport, (3) ekonomisk säkerhet, (4) indsatsberedskaber, (5) CBRN samt (6) koordinering av beredskapsplaneringe och kriskommunikation.
[78] Fakta blad, “Den civile sectors beredskab” samt BRS publikation ”Helhedsorienteret beredskabsplanlaegning, information, inspiration og praktik” [oktober 2005]

beredskapsnivåerna.[79] Under sikkerhedsudvalget finns ett Æmbetsmannaudvalg (ung. ”ämbetsmannautskottet”) som består av opolitiska departementschefer med uppgift att bereda underlag till sikkerhedsudvalget. Under dessa finns i sin tur Kriseberedskabsgruppen där avdelningscheferna ingår. Krisberedskapsgruppen arbetar i en krissituation efter den nationella beredskapsplanen som innehåller riktlinjer för hur den nationella nivån ska agera i en kris.[80]

Utöver krisledningsorganen finns även koordinationsforum på olika nivåer för att tillförsäkra samverkan under en kris. På central nivå har man t.ex. inrättat den nationella operativa staben under Rikspolisstyrelsen. Staben består av representanter för rikspolisstyrelsen (Rigspolitiet), försvaret (försvarskommandoen), Beredskabsstyrelsen, socialstyrelsen (sundhedsstyrelsen) samt efter behov andra civila myndigheter. Staben ska inte fatta beslut men har till uppgift att skapa en gemensam lägesbild och prioritering hos de olika aktörerna samt samordna insatser vid mycket stora händelser. Vidare har en Internationell operativ stab skapats år 2005 som en följd av tsunamin då mycket kritik riktades mot det danska Utrikesdepartementets hantering av katastrofen.[81] Under dessa staber finns slutligen de lokala staberna.[82] På lokal nivå ansvarar kommunen för att i princip alla uppgifter som kommunen har i fredstid också kan utföras under kris eller krig.[83] Vid större olyckor och katastrofer där det behövs tvärsektoriell samordning som inte den lokala nivån mäktar med på egen hand finns dock på regional nivå en koordineringsstab som leds av chefen för polisregionen. De regionala staberna är operativa och här ingår även representanter från andra myndigheter.[84]

I Danmark ansvarar Politiets Efterretningstjeneste, PET (motsvarande SÄPO) tillsammans med övrig polis, för att tillvarata Danmarks inre säkerhet och för den del av insatsen mot terrorism som utgörs av analys och efterforskningar efter personer eller grupper som kan misstänkas för brott enligt strafflagens terrorbestämmelser. I den s.k. Kontaktgruppe for Kontraterrorisme träffas ett flertal myndigheter regelbundet och PET

[79] Beredskapsnivåerna sträcker sig från ”allmän daglig beredskap” till ”fullt etablerad beredskap” enligt färgkoderna vit, grön, gul, orange och slutligen röd. Den 20 juli 2005 träffades utskottet för första gången med anledning av de hot som framfördes mot Danmark efter händelserna i London den 7 juli.

[80] Hittills har dessa fora fungerat lite omvänt eftersom den politiska nivån ofta träffats först och fattat vissa beslut fast att ämbetsmannagruppen egentligen är tänkt att rådge samt förse den politiska nivån med relevant underlag.

[81] Regeringens redegorelse om beredskabet, maj 2007. Den internationella staben är ett forum för samarbete och koordinering under internationella kriser som berör danskar i utlandet och består av de mest berörda myndigheterna. Staben kan allt efter krisens beskaffenhet utvidgas med relevanta myndigheter och privata aktörer som försäkrings- och resebolag.

[82] Regeringens redegorelse om beredskabet, maj 2007. Hur dessa staber ska verka tillsammans är dock fortfarande oklart.

[83] Kommunerna är enligt den danska Beredskabslagen skyldiga att inrätta beredskapsplaner för alla tjänster de ansvarar för såväl i fredstid som i krigstid eller kriser. Amterna, som ungefär motsvarar våra landsting, har t.ex. till uppgift att planera för att skadade kan behandlas även vid kris eller krig och polisen koordinerar ledningen vid alla blåljusinsatser såväl vid vardagsolyckor som vid stora olyckor och terroristattacker. Källa: International CEP Handbook (2006) Danmark s. 57-60 samt KBM:s landunderlag: Bilaga A Danmarks krishanteringssystem (ej publicerad)

[84] KBM:s landunderlag: Bilaga A Danmarks krishanteringssystem (ej publicerad)

samarbetar också med Statens Luftfartsvæsen och Søfartsstyrelsen samt de enskilda polisområdena kring säkerheten för den civila luftfarten och flygplatserna samt för hamnar, skepp och rederiers säkerhet. PET har också ett tätt samarbete med *Forsvarets Efterretningstjeneste* (FE) och underrättelsetjänsterna koordinerar insatser på ett antal områden. FE:s främsta uppgift är att samla in, analysera och förmedla information om förhållanden i utlandet av betydelse för Danmarks säkerhet.[85]

4.2 Inställning till direktivet för skydd av kritisk infrastruktur

För den nationella samordningen inför EPCIP-förhandlingarna tillsattes man i Danmark en koordineringsgrupp med deltagare från bl.a. utrikesministeriet, transport- och energiministeriet, energistyrelsen, familje- och konsumentministeriet, försvarsministeriet, Beredskabsstyrelsen, inrikes- och hälsovårdsministeriet, IT- och telestyrelsen, miljöstyrelsen, nationalbanken, Rikspolisstyrelsen samt den danska säkerhetstjänsten (Politiets Efterretningstjeneste).[86]

I Danmark har försvarsministeriet regelbundet underrättat Folketingets europautskott, försvarsutskott och rättsutskott om kommissionens förslag till direktiv om en kartläggning och klassificering av europeisk kritisk infrastruktur och bedömningen av behoven att stärka skyddet av denna. I officiella dokument från samrådet med den danska riksdagen framgår att den danska regeringen ställer sig positiv till EPCIP och ger sitt överordnade stöd för direktivförslaget. Den danska regeringen framhåller att det är regeringens målsättning att undvika att sårbarheter i en medlemsstat medför omfattande konsekvenser för andra medlemsstater och uppger att detta mål mest ändamålsenligt kan uppnås genom en koordinerad insats på europeisk nivå. Regeringen understryker dock att huvudansvaret för skyddet av kritisk infrastruktur ska ligga på medlemsstaterna och ägarna/operatörerna av kritisk infrastruktur. Regeringen betonar vidare vikten av att ett direktiv verkligen får ett mervärde och påpekar att många av de områden som kan komma att omfattas av direktivet redan är reglerade i nationell eller internationell lagstiftning. Från danskt håll framhålls vidare att man bör ha i åtanke att många medlemsstater redan har CIP-program som ligger före EPCIP både i form av erfarenhet och komplexitet. Den danska regeringen anser vidare att EPCIP-ramverket bör vara frivilligt och att nationell kritisk infrastruktur ska ligga utanför denna. Den danska regeringen framhåller också vikten av att kriterierna för utpekandet av kritisk infrastruktur preciseras närmare och att man verkar för att minimera risken för att onödiga administrativa bördor åläggs operatörer och myndigheter. Man framhåller i sammanhanget att det är viktigt att större ansträngningar läggs på att definiera ägarna och operatörernas rättigheter och skyldigheter och betonar att de danska ägarna

[85] KBM:s landunderlag: Bilaga A Danmarks krishanteringssystem (ej publicerad).
[86] Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007] + bilaga 1 den 4 januari 2006.

och operatörerna i remissvaren framhållit en ovilja att acceptera merkostnader för att skydda kritisk infrastruktur.[87]

Vad gäller inrättandet av säkerhetsplaner framhåller man från dansk sida att direktivets förslag om att all identifierad europeisk kritisk infrastruktur ska ha utarbetade OSP kan vara bra särskilt som en frivillig metodik för operatörer med liten erfarenhet på området. Dialogen med ägare och operatörer av europeisk kritisk infrastruktur anser man dock ska vara frivillig och bygga på utbyte av best practice. Danmark stödjer vidare inrättandet av en kontaktpunkt (CIP-Contact Point) utan auktoritet som lämnar det upp till medlemsstaterna att själva organisera denna uppgift.

Vad gäller förslaget om ett etablerande av ett informations- och varningssystemet framhåller man att CIWIN skulle kunna vara ett viktigt instrument för att stärka utbytet av erfarenheter och kunskapen om hur man analyserar hot och sårbarheter, inte minst mellan den offentliga och den privata sektorn, men att CIWIN inte ska ha någon roll i delandet av hot- och sårbarhetsinformation. Danmark anser således att t.ex. varningar och larm av nära förestående hot ligger utanför EPCIP-ramen.[88]

En sammanfattning av den danska privata sektorns inställning till EPCIP ger vid handen att de flesta ägare/operatörer av kritisk infrastruktur välkomnar direktivet. Bl.a. framhölls från flera håll att det är positivt att EU skapar en gemensam säkerhetsnivå för den kritiska infrastrukturen samtidigt som det är viktigt att se till att programmet minimerar de negativa konsekvenserna för konkurrensen. Det framhölls också att internationellt samarbete redan existerar och att det är viktigt att hänsyn tas till redan existerande åtgärder och principer. I ett remissvar framhölls att EPCIP endast borde fokusera på terrorism då existerande lagar och operatörers beredskapsplaner redan täcker andra typer av händelser. Det framhölls vidare att det var oacceptabelt att ägare/operatörer åläggs finansieringsbördan för eventuella utökade åtgärder.[89]

4.3 Bedömning av direktivets nationella konsekvenser

Vid en bedömning av direktivförslagets konsekvenser för statsfinanserna, samfundsekonomin, miljön och skyddsnivån konstaterades att ett antagande av direktivet i dess nuvarande utformning kommer att förpliktiga den danska staten att identifiera europeisk kritisk infrastruktur i landet samt kritisk infrastruktur utomlands som vid ett avbrott eller ödeläggelse skulle få

[87] Se ”Denmark´s response to the Green Paper on a European Programme for Critical Infrastructure Protection [30 januari 2006] samt [1 juli 2005] samt Regeringens redegorelse om beredskabet, maj 2007. Då varken Beredskabsstyrelsen eller det danska Försvarsdepartementet haft möjlighet att delta i studien bygger följande framställning endast på landets officiella dokument samt den skriftliga återrapporteringen från ProCiv-mötena.

[88] En närmare dansk hållning justeras i takt med den löpande utvärderingen av förslagets räckvidd kring de eventuella nationella administrativa, ekonomiska och lagstiftningsmässiga konsekvenserna. Regeringens redegorelse om beredskabet, maj 2007

[89] Annex – summary of responses from the Danish private sector och Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007].

väsentliga konsekvenser för Danmark.[90] Den danska bedömningen är dock enligt den öppna dokumentationen från samrådet med den danska riksdagen att många av de områden som kan komma att omfattas av direktivet redan är reglerade i nationell eller internationell lagstiftning.

Vid den nationella granskningen av gällande dansk rätt och direktivförslagets konsekvenser härför konstaterar man att ansvaret för skydd av kritisk infrastruktur i Danmark idag bygger på sektorsansvarsprincipen och att det är upp till de enskilda ministrarna inom deras område att planera för att kunna upprätthålla samhällets kritiska funktioner i händelse av olyckor och katastrofer.[91] Respektive ministerium ska vidare sörja för att nödvändig lagstiftning mm. införs i ressortlagstiftningen. Det finns i dagsläget m a o inga generella bestämmelser om skydd av kritisk infrastruktur även om det existerar en rad sektorsbaserade åtgärder inom sektorerna för IT, hälsa, finans, transport, den kemiska sektorn och den nukleära sektorn. Beredskapskrav till operatörer av kritisk infrastruktur finns bl.a. i Havnesikringsbekendtgørelsen, Elforsyningslovens § 85 b, Naturgasforsyningslovens § 15 a, Varmeforsyningslovens § 29 a, Lov om pligtige lagre af mineralolie og mineralolieprodukter § 5 a, Offshoresikkerhedslovens § 45, stk. 4-5, Fødevarelovens § 59, Sundhedsloven §§ 210-211, samt Lov om konkurrence og forbrugerforhold på telemarkedet § 86. Den danska bedömningen är att en implementering av kommissionens förslag till direktiv bl.a. kommer att kräva ändringar i dansk lag och att kravet om lagstiftning kan uppfyllas genom att relevanta bestämmelser införs i existerande sektorslagstiftning eller genom att det införs en särskild lagstiftning om europeisk kritisk infrastruktur. [92]

Från danskt håll har man konstaterat att ett eventuellt inrättande av ett europeiskt program för skydd av kritisk infrastruktur kommer att medföra en rad nya uppgifter men att det utifrån nuvarande underlag är svårbedömt att veta exakt hur omfattande dessa uppgifter kommer att bli. Man konstaterar dock att uppgifternas karaktär och omfång kommer att bero på de kriterier som ska råda för utpekandet av ECI samt att de utökade uppgifterna kommer att involvera alla myndigheter med ansvar för kritisk infrastruktur. Där tillkommer att arbetet med den övriga nationella kritiska infrastrukturen kan påverkas av det arbete som görs inom ramen för den europeiska kritiska infrastrukturen. Kravet i direktivförslaget om att ägare och operatörer av europeisk kritisk infrastruktur ska upprätta säkerhetsplaner (OSP) för en utpekad ECI kan komma att pålägga de utpekade verksamheterna ytterligare arbetsuppgifter och därmed extra utgifter. Man konstaterar dock även här att hur omfattande dessa åtaganden blir är avhängigt i vilken omfattning de uppställda kraven verkligen innebär ändrade och utökade uppgifter jämfört med det säkerhetsarbete som operatörerna redan idag utför. Man konstaterar att det i Danmark inom de olika sektorerna är stor skillnad på i hur hög grad

[90] Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007].
[91] Den danska Beredskabsloven § 24
[92] Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007] samt [11 januari 2007]

enskilda element i säkerhetsplanerna är omfattade av existerande sektorsspecifika krav. Därmed skiljer det sig också hur stora extra finansiella och administrativa bördor kravet på en standardiserad säkerhetsplan skulle innebära för olika operatörer av en europeiskt kritisk infrastruktur. Från danskt håll konstateras att de potentiella ekonomiska och administrativa bördorna för operatörerna minskas om kraven på innehållet i säkerhetsplanerna kan uppfyllas genom ett mindre tillägg i redan existerande beredskaps- och säkerhetsplaner.[93]

Då de danska representanterna inte haft möjlighet att delta i studien har det inte varit möjligt att närmare undersöka om några speciella förberedelser vidtagits för att förbereda för en eventuell implementering av EPCIP och direktivet.

4.4 Sammanfattning

Vid den danska bedömningen av direktivförslagets konsekvenser för statsfinanserna, ekonomin, miljön och skyddsnivån konstaterades i generella termer att ett antagande av direktivförslaget kommer att medföra en rad nya uppgifter men man konstaterade samtidigt att det utifrån nuvarande underlag är svårbedömt att veta exakt hur omfattande dessa uppgifter kommer att bli. Den danska uppfattningen är enligt officiella dokument från samrådet med den danska riksdagen att många av de områden som kan komma att omfattas av direktivet redan är reglerade i nationell eller internationell lagstiftning. Vad gäller förekomsten av OSP och SLO konstaterades att det inom de olika sektorerna råder stor skillnad på i hur hög grad enskilda element i säkerhetsplanerna är omfattade av existerande sektorsspecifika krav. Därmed blir det också svårbedömt exakt hur stora finansiella och administrativa bördor kravet på exempelvis säkerhetsplaner skulle innebära för ägare och operatörer av utpekad europeisk kritisk infrastruktur. Den danska bedömningen är att en implementering av kommissionens förslag till direktiv kommer att kräva ändringar i dansk lag. Då de danska representanterna inte haft möjlighet att delta i studien har det dock inte varit möjligt att närmare undersöka om några speciella förberedelser vidtagits för detta syfte.

[93] Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007]

5 FINLAND

I nedan sektion ges en översiktlig beskrivning av Finlands arbete med skydd av kritisk infrastruktur med fokus på vad man definierar som kritisk infrastruktur, hur ansvars- och ledningsstrukturer ser ut, vilken roll de lokala myndigheterna, departementen och andra centrala aktörer har samt hur CIP-åtgärder finansieras. Avsnittet avslutas med en sammanfattning av den finska synen på EPCIP och vilka förberedelser som har vidtagits för ett eventuellt direktiv på området.

Förkortningar

ACIS	Advisory Committee for information Security
FBC	Försörjningsberedskapscentralen (Fi. Huoltovarmuuskeskus, HVK) (Eng. National Emergency Supply Agency, NESA)
FEP	Den försvarsekonomiskaplaneringskommissionen (Fi. Puolustustaloudellinen suunnittelukunta, PTS (Eng. The National Board of Economic Defence, NBED)
FICORA	Den finska kommunikationsregleringsmyndigheten
UTVA	Regeringens utrikes- och säkerhetspolitiska utskott
TPAK	Säkerhets- och försvarskommittén (Fi. Turvallisuus ja puolustusasiain komitea)
TSVF	Strategin för tryggandet av samhällets livsviktiga funktioner
VAHTI	Ledningsgruppen för datasäkerhet inom statsförvaltningen (Fi. Valtionhallinnon tietoturvallisuuden johtoryhmän) (Eng. The Steering Committee for Data Security in State Administration)

5.1 Landets arbete med skydd av kritisk infrastruktur

I Finland började man jobba med skydd av kritisk infrastruktur redan 1995 då skydd av kritisk infrastruktur inkorporerades i det övergripande totalförsvarskonceptet.[94] I Finland pratar man om *vital infrastruktur* och betonar särskilt en för samhällsverksamheten nödvändig funktionshelhet.

Mot bakgrund av behovet att säkra samhällets funktioner, höja informationssäkerheten och stärka skyddet av kritisk infrastruktur fick för ett antal år sedan en säkerhets- och försvarskommitté i uppdrag att arbeta fram en nationell strategi. Som en följd av detta antog Finland i november

[94] Även om man inte använde sig av just detta begrepp motsvarade själva innehållet det man åsyftar när man talar om skydd av kritisk infrastruktur.

2003 *Strategin för tryggande av samhällets livsviktiga funktioner*.[95] I strategin identifieras sju samhällsviktiga funktioner: (1) Ledning av staten, (2) internationell verksamhet, (3) det militära försvaret av riket, (4) upprätthållande av den inre säkerheten, (5) ekonomins och infrastrukturens/samhällets funktionsförmåga, (6) befolkningens utkomstkydd och handlingsförmåga samt (7) mental kristålighet.[96]

Tabell: Sammanställning över samhällsviktiga funktioner

Samhällsviktig funktion	Ansvarigt departement
1. Ledning av staten	Premiärministerskansliet och Justitiedepartementet
2. Internationell verksamhet	Utrikesdepartementet
3. Det militära försvaret av riket	Försvarsdepartementet
4. Upprätthållande av den inre säkerheten	Inrikesdepartementet
5. Ekonomins och samhällets funktionsförmåga	Finansdepartementet, Handels- och industridepartementet, Transport- och kommunikationsdepartementet
6. Befolkningens utkomstskydd och handlingsförmåga	Socialdepartementet, Utbildningsdepartementet
7. Mental kristålighet	Jordbruksdepartementet, Finansdepartementet

Källa: International CEP Handbook (2006) Finland, s. 68 samt Strategin för tryggande av samhällets livsviktiga funktioner (2006).

I strategin för tryggandet av samhällets livsviktiga funktioner beskrivs för varje funktionsförmåga hur ett så kallat måltillstånd ska kunna upprätthållas i alla situationer. Utifrån måltillståndet organiserar därefter de ansvariga ministerierna den prestationsförmåga som krävs för att upprätthålla de livsviktiga funktionerna. Detta innebär att varje ministerium leder beredskapen och utvecklandet av den lagstiftning som rör sitt förvaltningsområde. Eftersom de sju identifierade vitala samhällsfunktionerna sträcker sig över flera ministerier och sektorer är dock de andra ministerierna skyldiga att stödja detta arbete.[97] Kansli- och beredskapschefsmötena stöder det behöriga ministeriet i egenskap av samordnande organ och Försörjningsberedskapscentralen verkar i samarbete med alla förvaltningsområden som sakkunnig och genomförare av planeringen och den operativa verksamheten i fråga om upprätthållandet och utvecklandet av försörjningsberedskapen.[98]

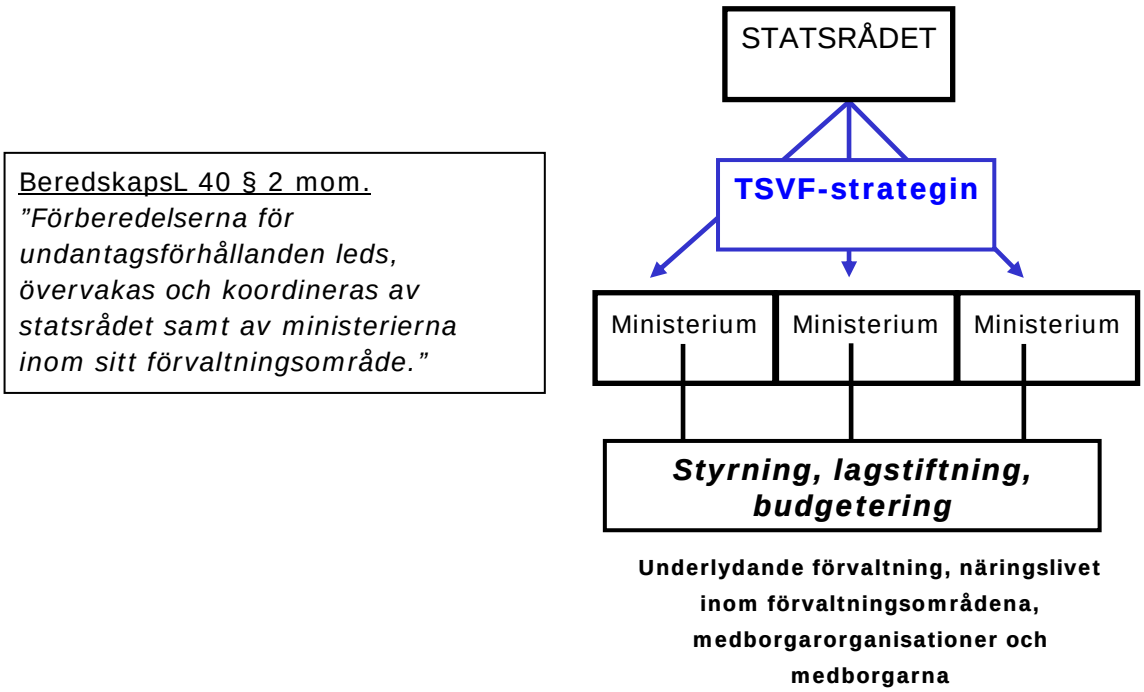
[95] Strategin för tryggandet av samhällets livsviktiga funktioner (TSVF) utarbetades för första gången år 2003 och har sedan förnyats genom statsrådets principbeslut den 23 november 2006. Informationen och samordningen av grunderna för beredskapen i strategin gäller inte bara myndigheterna utan även näringslivet och medborgarorganisationerna. Säkerhets- och försvarskommittén ansvarar för översynen av principbeslutet.

[96] Elektronisk information och kommunikationssystem har identifierats som en speciellt viktig del av samhällets funktionsförmåga. I strategin för tryggande av samhällets vitala funktioner listas således också hot mot informations- och kommunikationssystem först. Det var även dessa områden som framhölls i regeringens försvars- och säkerhetspolitiska policyrapport som presenteras var fjärde år till parlamentet.
CIIP Handbook (2006) Finland s. 86

[97] Principen är dock inte bindande och det finns inga sanktioner i händelse av att delar av förvaltningen inte skulle följa strategin. Detta upplevs dock inte som ett problem då det inom den finska förvaltningen anses räcka med ett ”peer pressure” samt möjligheten för att utsättas för kritik från premiärministern. Genom att den finska statsförvaltningen är relativt liten så känner de flesta aktörerna dessutom varandra.

[98] Strategin för att tryggande av samhällets livsviktiga funktioner (2006)

Figur: Den finländska strategin för tryggande av samhällets vitala funktioner



Kommentar: TSFV står för strategin för tryggande av samhällets vitala funktioner. Ministerierna ska beakta TSVF-strategins riktlinjer i styrningen av förvaltningsområdena och i lagstiftningsarbetet. Säkerhets- och försvarskommittén ansvarar för den gemensamma uppföljningen av genomförandet av strategin tillsammans med beredskapschefsmötet.
Källa: Strategin för tryggande av samhällets livsviktiga funktioner (2006) s.5

Även om strategin för skyddet av kritisk infrastruktur utgår ifrån en bred syn på hot och risker (en s.k. all-hazards approach) har man i Finland på senare tid börjat lyfta fram tekniska och specifikt informationstekniska infrastrukturer lite mer.[99] I Finland arbetar främst tre myndigheter med skydd av kritisk informationsinfrastruktur (CIIP); (1) den finska kommunikations- och regleringsmyndigheten (FICORA) som fokuserar på stärkande av informationssäkerhet, teknisk reglering, och standardisering, (2) Försörjningsberedskapscentralen (FBC) som har till uppgift att analysera hot och risker mot kritisk informationsinfrastruktur och slutligen (3) ledningsgruppen för datasäkerhet inom statsförvaltningen (VAHTI) vilka utarbetar policy riktlinjer och praktiska guider för informationssäkerhetssystem.[100]

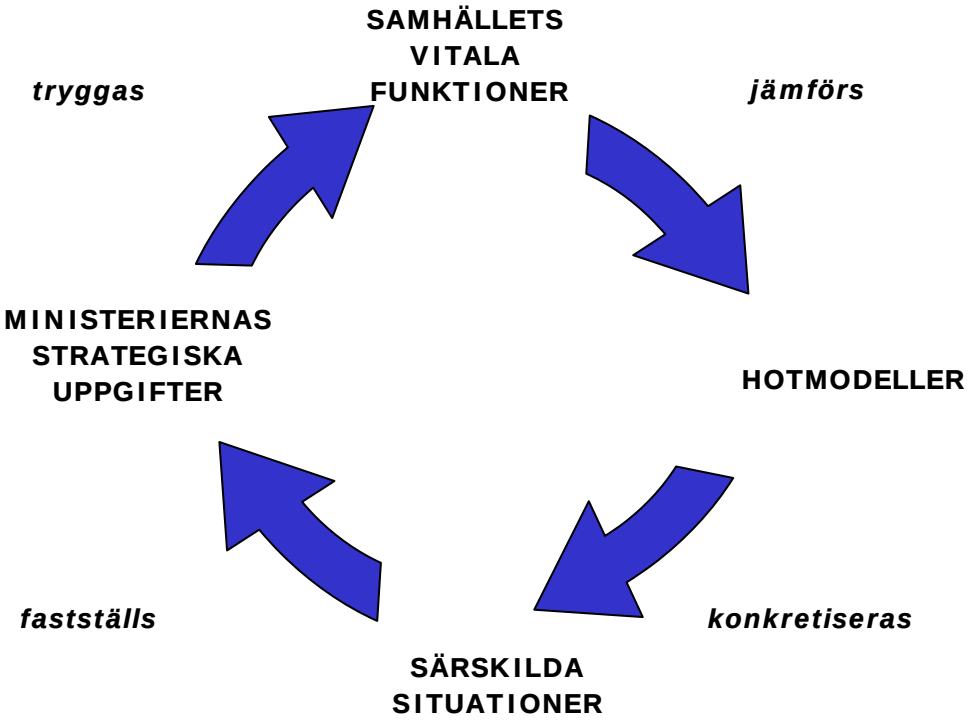
[99] Hagelstam, (2005) Försörjningsberedskapscentralen s.8-11
[100] Ledningsgruppen för datasäkerhet inom statsförvaltningen (VAHTI) är en grupp av experter underordnade Finansministeriet vars främsta uppgift är att ta fram riktlinjer för datasäkerhet och informationshantering. VAHTI har bl.a. publicerat ett flertal praktiska guider om informationssystemssäkerhet riktade främst till statsadministrationen men som även många privata organisationer har använt sig av. CIIP Handbook (2006), Finland, s. 91

I strategin för tryggandet av samhällets vitala funktioner[101] beskrivs även de hotbilder som äventyrar de vitala funktionerna och för varje situation har man utsetts ett ministerium som i första hand ansvarar för beredskapen och hanteringen av situationen.[102] Generella regler för förberedelser inför en krissituation finns i ”The Emergency Power Act” och ”The Readiness Act” som stipulerar att myndigheter på alla nivåer genom kontinuitetsplanering och andra förberedande åtgärder ska vara förberedda på att kunna upprätthålla deras skyldigheter även under en krissituation.[103] I samband med allvarliga störningar och i undantagsförhållanden behöver myndigheterna speciella befogenheter för att kunna trygga samhällets livsviktiga funktioner. De mest centrala specialbefogenheterna finns fastslagna i beredskabslagen (1080/1991). För de mest allvarliga kriserna har man stiftat lagen om försvarstillstånd (1083/1991), med vilken landet eller delar därav kan försättas i försvarstillstånd. I försvarstillstånd kan de militära myndigheterna ge order om tryggandet av verksamhetsförutsättningarna för landets militära försvar.[104] För beredskapen och inledandet av verksamheten använder de behöriga myndigheterna de rätt så omfattande befogenheter som lagstiftningen ger dem i fråga om normala förhållanden.[105]

Även företag och organisationer deltar i samordningen av åtgärder för att skydda den vitala infrastrukturen. Utgångspunkten i företagens beredskap är de affärsmässiga grunderna, de avtal som ingåtts med kunder samt den riskhantering som hänför sig till dessa. I den mån beredskapen inte är tillräcklig ur samhällssynpunkt kan beredskapsansvaret utökas genom inrättandet av lagstadgade skyldigheter. Kostnaderna för beredskapen kan då ersättas med offentliga medel i särskilt angivna fall. De lagstadgade beredskapsskyldigheterna får inte störa verksamheten och de jämlika konkurrensförutsättningarna på marknaden.[106]

[101] Principbeslutet om en strategi för tryggande av samhällets vitala funktioner är ett styrdokument som statsrådet har fastställt för ministerierna. Beslutet konkretiserar den säkerhets- och försvarspolitiska redogörelsen och kompletterar andra styrdokument av statsrådet som behandlar olika delområden av säkerheten. Genom strategin samordnar man de åtgärder som behövs för beredskapen inom förvaltningsområdena och för tryggande av de vitala funktionerna.
[102] Hotbilderna beskrivs i bilaga 1 i strategin för tryggandet av samhällets vitala funktioner. I bilaga 2 beskrivs de ministerier som ansvarar för beredskapen.
[103] International CEP Handbook (2006) Finland s. 69.
[104] Försörjningsberedskapscentralen, FBC
[105] Under undantagsförhållanden kan statsrådet med riksdagens samtycke ges rätt att använda ytterligare befogenheter enligt beredskapslagen. Strategin för att tryggande av samhällets livsviktiga funktioner (2006)
[106] Strategin för tryggande av samhällets livsviktiga funktioner (2006) samt intervju med tjänsteman vid Försörjningsberedskapscentralen [16 januari 2008].

Figur: Strategins uppbyggnad



Kommentar: Figuren beskriver principen för tryggande av de vitala funktionerna i samhället.
Källa: Strategi för tryggande av samhällets livsviktiga funktioner (2006) s. 4

I tryggandet av samhällets vitala funktioner ingår åtgärder både under beredskapstiden och sedan en kris har brutit ut. I Finland skiljer man på normala förhållanden, störningssituationer och undantagsförhållanden. Under normala förhållanden är tyngdpunkten i tryggandet av de vitala funktionerna förlagd till förebyggandet, bekämpningen och hanteringen av olika slags hot samt återhämtningen från konsekvenserna av dessa hot med stöd av den gällande lagstiftningen och de disponibla resurserna under normala förhållanden. I störningssituationer ska de behöriga myndigheterna, och vid behov statsledningen, vidta särskilda åtgärder för att klara av situationen. Störningssituationer kan exempelvis medföra ibruktagande av befogenheter som ingår i författningar som gäller under normala förhållanden, omfördelning av anslag, personalarrangemang och anvisande av andra tilläggsresurser samt översyn av författningar. I störningssituationer är det viktigt att samarbetet intensifieras och ledningsförutsättningarna tryggas. I synnerhet betonas vikten av att en lägesbild sammanställs och att den upprätthålls, analyseras och distribueras till dem som behöver den. I en störningssituation är det viktigt att aktivt informera om situationen, myndigheternas verksamhet och förhållningsregler samt statsledningens riktlinjer. Bestämmelser om undantagsförhållanden ingår i beredskapslagen och lagen om försvarstillstånd. De befogenheter som fastställs i lagarna kan endast tas i bruk i situationer som myndigheterna inte kan få kontroll över med normala befogenheter.[107]

[107] Strategin för att tryggande av samhällets livsviktiga funktioner (2006)

En viktig aktör involverad i skydd av kritisk infrastruktur är Försörjningsberedskapscentralen (FBC).[108] FBC har en växande roll på området skydd av kritisk infrastruktur då man både utvecklar och finansierar tekniska back-up-system. FBC arbetar även tillsammans med den försvarsekonomiska planeringskommissionen (FEP)[109] med att analysera hot och risker och huvudfokus ligger idag till stor del på kritisk infrastruktur där informationssäkerhet och skydd av olika IT system prioriteras. FBC och FEP utformar också planer och riktlinjer för myndigheter och företag vad gäller hantering och kontroll av hot och risker.[110]

Ända sedan kriget har man i Finland haft ett privatoffentligt samarbete som sammanför statliga myndigheter och privata aktörer i krisberedskapsfrågor. Utöver Försörjningsberedskapscentralen (FBC) som är ett operativt, tväradministativt organ som i samverkan med näringslivet arbetar med försörjningsberedskapsfrågor är försvarsekonomiska planeringskommissionen (FEP) en annan framstående aktör. FEP:s uppgift består i att analysera hot mot det moderna nätverkssamhället, landets försörjning och vilka nödvändiga åtgärder för hantering av hoten som bör vidtas. FEP främjar även företagens beredskapsplanering genom att göra upp planer och anvisningar som förvaltningen sedan förverkligar i störningssituationer. Det privatoffentliga partnerskapet framträder bäst i FEP:s poolorganisation där poolerna ansvarar för den operativa beredskapen. Poolernas uppgift är bl.a. att tillsammans med företagen följa upp, utreda, planera och förbereda åtgärder för utveckling av de egna branschernas försörjningsberedskap.[111]

5.2 Inställning till direktivet för skydd av kritisk infrastruktur

Den finländska regeringens ståndpunkt är att huvudprinciperna i direktivförslaget är bra och regeringen stödjer att man inom EU diskuterar skyddet och betydelsen av kritisk infrastruktur. Från finländskt håll anser man dock att kartläggningen och klassificeringen av kritisk infrastruktur och bedömningen av behovet av skydd ska ligga hos medlemsstaterna med beaktande av subsidiaritetsprincipen. Regeringen anser att programmet för skydd av kritisk infrastruktur endast ska vara riktgivande men däremot anser man att kriterierna för kartläggning av objekt som omfattas av programmet samt förfarandet vid klassificeringen och bedömningen av behovet av extra skydd genomförs genom ett direktiv som är förpliktande

[108] Försörjningsberedskapscentralen (FBC) är en statlig myndighet som bildades 1993 som sorterar under Handels- och industriministeriet. FBC har till uppgift att planera och handha den operativa verksamheten som behövs för att upprätthålla och utveckla landets försörjningsberedskap. Tyngdpunkten ligger vid att säkerställa de tekniska systemen. Speciellt stor uppmärksamhet fästs vid samhällets kritiska informationssystem. Försörjningsberedskapscentralen (FBC).

[109] Den försvarsekonomiska planeringskommissionen (FEP) inrättades 1955 och lyder under Handels- och industriministeriet. FEP är ett nätverk av kommittéer bestående av ledande experter från såväl det offentliga som det privata. Statsrådet utnämner FEP för fyra år i taget och den löpande planeringsperioden täcker åren 2004–2008. Uppemot 800 personer arbetar för närvarande på FEP. CIIP Handbook (2006), Finland, s. 91

[110] CIIP Handbook (2006), Finland, s. 90

[111] Försörjningsberedskapscentralen (FBC)

för medlemsländerna. Från finländskt håll framhålls att även om man har kommit olika långt i olika länder och vidtagit olika och varierande åtgärder så måste infrastrukturägarna generellt höja säkerheten och man menar att det behövs en bindande lag för att uppnå detta.[112]

Ett av de främsta mervärdena med just en gemensam EU-ram på området är enligt finländarna att konkurrensen på marknaden inte störs. Då de flesta infrastrukturägare är privata och åtgärder för att höja säkerheten kring den kritiska infrastrukturen sannolikt leder till ökade kostnader anser man att dessa ska vara lika för alla infrastrukturägare i alla länder så att ingen missgynnas. Om grunderna för identifieringen och klassificeringen av objekt inom den kritiska infrastrukturen på EU-nivå stärks genom en bindande rättsakt, garanteras med andra ord ett jämlikt och enhetligt förhållningssätt och förfarande medlemsländerna emellan. Om kriterierna endast var riktgivande, skulle förfaringssättet i de olika medlemsländerna sannolikt variera.[113]

I dagsläget är inga artiklar problematiska för finskt vidkommande och generellt sett är man ganska nöjda med innehållet i direktivet.[114] Som det ser ut nu anser man att det största problemet är att klara ut definitionen av kritisk infrastruktur och vilka kriterier som ska gälla. Finland stödjer här kommissionens förslag och förespråkar att en kritisk infrastruktur ska beröra två medlemsstater för att betecknas som europeisk kritisk infrastruktur (ECI). Om definitionen skulle utgå ifrån tre medlemsstater så menar man att direktivet inte alls kommer att beröra Finland och ett färre antal utpekade ECI menar man skulle försvåra möjligheten att uppnå direktivets initiala syfte.[115]

Den finländska regeringen stöder också de skyldigheter som åläggs ägarna och operatörerna av en ECI i fråga om utarbetande av säkerhetsplaner (OSP), vidarebefordran av planerna till medlemsstaternas myndigheter samt utnämningen av sambandsansvariga i säkerhetsfrågor (SLO). Man framhåller dock samtidigt att det är viktigt att de skyldigheter som åläggs verksamhetsutövarna genom direktivet inte innebär skyldigheter som är betydligt mer betungande för de finländska verksamhetsutövarna än för närvarande.[116]

Enligt den finländska representanten är de privata ägarna och operatörerna i landet varse om vad som pågår på området och i och med att konkurrensen

[112] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[113] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007] samt statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Helsingfors den 7:e juni 2007
[114] Till en början var man dock från finskt håll skeptiska till förslaget att ge kommissionen auktoritet att ta beslut om individuella infrastrukturobjekt som det första utkastet till direktiv föreslog.
[115] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007] samt kommunikationsutskottets utlåtande kring statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Dokumentreferens:8/2007 rd. Helsingfors den 28 september 2007
[116] Kommunikationsutskottets utlåtande kring statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Dokumentreferens:8/2007 rd. Helsingfors den 28 september 2007

inte påverkas har dessa i de flesta fall heller inga invändningar mot direktivet. De privata ägarna och operatörerna avvaktar nu vad direktivet kommer att medföra i mer precisa termer. Något som särskilt betonas inför den fortsatta behandlingen av frågan är att den privata sektorn måste vara involverad i förberedelserna och implementeringen av direktivet.[117]

5.3 Bedömning av direktivets nationella konsekvenser

I Finland har man inte gjort någon nationell konsekvensanalys men man förutser heller inga större förändringar till följd av direktivet. I dagsläget har man redan en nationell strategi för att säkerställa vitala funktioner i samhället och denna inkluderar även skydd av kritisk infrastruktur. I strategin för tryggandet av samhällets vitala funktioner har man exempelvis pekat ut sju olika sektorer inom vilka man sedan har identifierat kritisk infrastruktur. Denna övergripande CIP-strategi uppdateras vart tredje eller fjärde år då alla regeringar, efter att samma objekt studerats om igen, antar en ny strategi och bestämmer vilka åtgärder som behöver vidtas just då. Med tanke på kontinuitetsplaneringen som redan görs inom ramen för detta arbete så bedömer man inte att direktivet kommer att medföra några större förändringar, men man betonar att det givetvis beror på hur långtgående idéer kommissionen har och vad man tillslut får igenom. Från finländskt håll har man uppfattningen att liknande system redan verkar finnas i många länder och att åtagandena som ett direktiv kan medföra inte lär bli så extremt dyra eller medföra några dramatiska förändringar. Som en följd av denna bedömning har man inte heller vidtagit några särskilda åtgärder för att förbereda för en eventuell implementering av ett direktiv. Från finländskt håll uppger man sig dock ha en generell idé kring vad direktivet kommer att innebära och hur man ska gå tillväga rent praktiskt för att genomföra ett eventuellt direktiv.[118]

Vad gäller utpekandet av potentiell europeisk kritisk infrastruktur i landet har man inte haft någon central diskussion om detta givet att kriterierna för identifieringen ännu inte är fastslagna. Den finländska representanten spånar kring att det kanske finns något transport- eller telekommunikationssystem mellan Finland och Sverige eller möjligtvis något på energiområdet som kan komma att bli utpekat som europeiskt kritisk infrastruktur men generellt framhåller man att situationen i Norden skiljer sig ganska mycket från den i Centraleuropa där länderna är sammankopplade med varandra på ett helt annat sätt.[119]

Vad gäller risk- och sårbarhetsanalyser genomför man i Finland redan liknande risk- och sårbarhetsanalyser som direktivet föreskriver då alla administrationer och myndighet ansvarar för att upprätta beredskapsplaner kring deras verksamhet.[120] I beredskapsplanerna bör exempelvis finnas en plan för hur verksamheten ska fortgå vid en exceptionell situation. Det finns

[117] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[118] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[119] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[120] Räddningstjänstmyndigheter och ägare av kritisk infrastruktur har exempelvis en skyldighet att upprätta kontinuitetsplaner och i den privata sektorn pratar man om ”business continuity plans”.

inte något generellt straff om företagen inte lyder dessa lagar, men i de fall det rör sig om lagstadgade skyldigheter kan ägaren/operatören beordras att lyda gällande regler genom hot om böter. I Finland är det Försörjningsberedskapscentralen (FBC) och den försvarsekonomiska planeringskommissionen (FEP) som har kontinuerliga kontakter med den privata sektorn och hjälper aktörerna att upprätta säkerhetsplaner, genomföra risk och sårbarhetsanalyser etc.[121] Den finländske representanten sammanfattar att förekomsten av säkerhetsplaner varierar från sektor till sektor men att man trots det har gjort bedömningen att den viktigaste kritiska infrastrukturen som telekommunikationer, energi och transport har grundläggande säkerhetsplaner och kontinuitetsplaner. Samma bedömning gjordes av kommunikationsutskottet då de lämnade sitt officiella utlåtande på direktivförslaget. Utskottet menar att det enligt de uppgifter de erhållit inte föreligger något problem med att lämna information och utforma planer i enlighet med det liggande direktivförslaget. Den övergripande bedömning var därmed att Finlands beredskapsförfarande inte kommer att påverkas ifall direktivet träder i kraft då de nuvarande beredskapsarrangemangen redan täcker in de åtgärder för kritisk infrastruktur som ingår i direktivförslaget.[122]

Samma sak gäller sambandsansvariga i säkerhetsfrågor (SLO) där den finländske representanten berättar att det oftast finns en utsedd person på företagen som ansvarar för upprättandet av säkerhetsplaner och kontinuitetsplaner även om dessa kan vara organiserade på olika sätt.[123]

Någon utvärdering av de totala ekonomiska konsekvenserna av ett direktiv på området har inte gjorts men den preliminära finska bedömningen är att det inte kommer att bli särskilt kostsamt för den finska staten trots att man har en princip om att ägarna/operatörerna bara behöver se till att skydda sin verksamhet till en nivå som är affärsmässigt nödvändig. Detta innebär att om staten ålägger dem ett ansvar att vidta ytterligare skyddsåtgärder så bekostas/delfinansieras dessa av staten och FBC. Man har inte diskuterat huruvida staten även fortsättningsvis ska täcka en del av merkostnaderna för skydd av kritisk infrastruktur om ett direktiv blir aktuellt. Det är till stor del avhängigt vad direktivet ålägger ägarna/operatörerna för uppgifter och skyldigheter.[124]

I statsrådets skrivelse till den finska riksdagen gällande rådets förslag till direktiv berörde man vidare vilka konsekvenser inrättandet av en CIP-kontaktpunkt skulle medföra men slutsatsen som drogs var endast att uppgifterna för såväl de nationella kontaktpunkterna som verksamhetsutövarnas kontaktpersoner var nya och eventuellt kunde leda

[121] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]. Den privata sektorn är indelad i uppemot 13-14 olika pooler där man handskas med sektorsspecifika problem och frågor.
[122] Kommunikationsutskottets utlåtande kring statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Dokumentreferens:8/2007 rd. Helsingfors den 28 september 2007
[123] Intervju, tjänsteman vid finska Inrikesdepartementet[14 december 2007]
[124] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]

till ett ökat resursbehov.[125] I Finland har man inte fattat något beslut om var kontaktpunkten i CIP-frågor kommer att ligga men inställningen är att detta kan organiseras rätt lätt. Som det ser ut nu så har man tre kontaktpersoner för CIP-frågor – en på försörjningsberedskapscentralen och två inom Inrikesdepartementet. Enligt intervjupersonen skulle den CIP Contact Point som omnämns i direktivet möjligtvis kunna komma att kopplas till FBC eller organiseras inom Inrikesdepartementet (alternativt Handels- och industriministeriet).[126] FBC uppger att de i sina kontakter med Inrikesdepartementet har framhållit att de anser sig vara lämpade för rollen.[127]

Vad gäller konsekvenser på lagstiftningsområdet har man i Finland gjort bedömningen att genomförandet av direktivet i viss mån kommer att förutsätta ändringar i den sektorsvisa lagstiftningen även om det inom vissa sektorer redan ingår motsvarande skyldigheter i lagstiftningen.[128] Detta gäller bl.a. den finska ”Emergency Power Act” och relaterad lagstiftning som rör den planeringsskyldighet som åläggs företagen. Inga förberedelser har dock vidtagits för detta syfte.[129] Den finska bedömningen är att skyldigheterna för nationella myndigheter och privata företag inom olika sektorer som förslaget till direktiv berör samt konsekvenserna för lagstiftningen behöver utredas närmare i den fortsatta beredningen.[130]

5.4 Sammanfattning

I Finland förutser man inga större förändringar på det nationella planet till följd av direktivet utan säger att de flesta ägare och operatörer redan har säkerhetsplaner och sambandsansvariga i säkerhetsfrågor (även om man inte benämner dessa som just Security Liaison Officers). I dagsläget arbetar man i Finland efter en nationell strategi för att säkerställa vitala funktioner i samhället och denna inkluderar även skydd av kritisk infrastruktur. Från finskt håll har man uppfattningen att liknande system redan verkar finnas i många länder och att åtagandena som ett direktiv kan medföra inte lär bli så extremt dyra eller medföra några dramatiska förändringar. Som en följd av denna bedömning har man inte heller vidtagit några särskilda åtgärder för att förbereda för en eventuell implementering av ett direktiv. I Finland har man inte gjort någon nationell konsekvensanalys av direktivet men man säger sig dock ha en generell idé kring vad det kommer att innebära och hur man ska gå tillväga rent praktiskt.

---

[125] Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur), Helsingfors den 7 juni 2007.
[126] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[127] Intervju, tjänsteman vid Försörjningsberedskapscentralen, FBC [16 januari 2008]
[128] Bland annat teleoperatörer och finansbranschen är underställda lagstadgad beredskap och rapporterar på ett liknande sätt som direktivet stipulerar till en övervakande myndighet. Inom andra sektorer har man avtalsbaserade planeringsskyldigheter; till exempel utför handelns centralaffärer ett omfattande beredskapsarbete utan lagstadgade skyldigheter.
[129] Intervju, tjänsteman vid finska Inrikesdepartementet [14 december 2007]
[130] Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur), Helsingfors den 7 juni 2007.

Någon utvärdering av de totala ekonomiska konsekvenserna av ett direktiv på området har inte gjorts men den preliminära finska bedömningen är att det inte kommer att bli särskilt kostsamt för staten trots att man i Finland har en princip om att ägarna/operatörerna bara behöver se till att skydda sin verksamhet till en nivå som är affärsmässigt nödvändig och att ytterligare skyddsåtgärder indirekt delfinansieras av staten och Försörjningsberedskapscentralen. Man har inte diskuterat huruvida staten även efter en eventuell implementering av EPCIP ska kompensera ägarna och operatörerna för eventuella merkostnaderna till följd av åtgärder för att skydda utpekad europeisk kritisk infrastruktur.

6 NEDERLÄNDERNA

I nedan sektion ges en översiktlig beskrivning av Nederländernas arbete med skydd av kritisk infrastruktur med fokus på vad man definierar som kritisk infrastruktur, hur ansvars- och ledningsstrukturer ser ut, vilken roll de lokala myndigheterna, departementen och andra centrala aktörer har samt hur CIP-åtgärder finansieras. Avsnittet avslutas med en sammanfattning av den holländska synen på EPCIP och vilka förberedelser som har vidtagits för en eventuell implementering av ett direktiv.

Förkortningar

AIVD	Den nederländska underrättelse- och säkerhetstjänsten (Algemene Inlichtingen- en Veiligheidsdienst)
BZK	Nederländska Inrikesdepartementet (Binnenlandse Zaken en Koninkrijksrelaties, BZK)
ERC	Expertisecentrum Risico- en Crisiscommunicatie
NAVI	Det nationella rådgivningscentret för skydd av kritisk infrastruktur (Nationaal Adviescentrum Vitale Infrastructuur)
NCC	Nationaal CrisisCentrum
NCTb	National Coordinator for Counter terrorism
NHTCC	National High Tech Crime Center
SOVI	Strategisch Overleg Vitale Infrastructuur
TNO	The Netherlands Organisation for Applied Scientific Research

6.1 Landets arbete med skydd av kritisk infrastruktur

I Nederländerna betraktas skydd av kritisk infrastruktur som en vital del av den nationella säkerheten. Man brukar säga att det är Nederländernas geografiska läge som har satt sin prägel på landets arbete med skydd av kritisk infrastruktur och syftar då på det utsatta läget invid Nordsjön, de stora floderna som flyter igenom landet, det inklämda läget mellan Tyskland och Belgien samt befolkningstätheten.[131] På senare tid har även det nederländska deltagandet i militära operationer utomlands samt de nära banden till USA gjort landet speciellt utsatt för terrorattentat vilket har fått landet att speciellt prioritera just skyddet av den kritiska infrastrukturen. Arbetet med att ta fram en övergripande holländsk nationell strategi för skydd av kritisk infrastruktur började år 1999 då man började planera för ett haveri av ICT inför millennieskiftet (Y2R).[132] Ända sedan dess har Nederländerna riktat speciellt fokus mot just skydd av kritisk infrastruktur.

[131] Nederländerna är t.ex. som genomfartsland en stor europeisk knutpunkt genomkorsat av vägar, järnvägar och floder. Krisberedskap i omvärlden – samordningsstrukturer i fem länder (2003) s. 40 KMB:s temaserie (2003:3)

[132] Utöver millennieskiftet har erfarenheterna från andra allvarliga händelser som t.ex. flygplanskraschen i Bijmelmeer utanför Amsterdam 1992, katastrofbränderna i Enschede

I Nederländerna är regeringen ansvarig för tillgänglighet och integritet i de flesta kritiska sektorerna och i de flesta fall är detta lagstiftat eller reglerat på annat sätt.[133] Nederländerna saknar självständiga myndigheter direkt under de tretton ministerierna. Ministerierna är istället mycket stora och delas in i direktorat. Respektive minister utövar s.k. ministerstyre och varje ministerium leds på tjänstemannanivå av en generaldirektör. I Nederländerna ansvarar Inrikesdepartementet (BZK) för samordningen av skydd av kritisk infrastruktur.[134] Utöver det övergripande policy ansvaret för CIP-frågor ansvarar Inrikesdepartementet för att koordinera CIP-policies mellan olika sektorer och ministerier samt internationellt. Mellan 2002-2004 ansvarade NCC (the National Coordination Center) för koordineringen av det holländska CIP-arbetet men sedan september 2004 har ansvaret flyttats över till The Directorate of Crisis Management som lyder under Inrikesdepartementet.[135] Sedan några år tillbaka finns också en avdelning som arbetar speciellt med att förbättra och utveckla kriskommunikationen; Expertise Centre for Risk and Crisis Communication (the ERC). Inrikesdepartementets expertcentrum för risk- och kriskommunikation kan också agera talesperson på regeringens vägnar vid kriser samt stötta lokala myndigheter med expertstöd vid kriser. Som det är idag fungerar ERC som en ”jourhavande kriskommunikatör”, med uppdrag flera gånger i veckan åt lokala myndigheter vid olika typer av kriser. Vid ERC är medarbetarna kontaktpersoner mot 3-4 regioner var.

Den nederländska underrättelse- och säkerhetstjänsten (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) utgör en annan del av Inrikesdepartementet och ansvarar specifikt för att skydda informationssäkerheten och vitala sektorer i det nederländska samhället. AIVD är också ansvariga för att analysera möjliga hot riktade mot de holländska CI-sektorerna. NHTCC (The National Hightech Crime Center) är vidare ett initiativ av den holländska polismyndigheten, Inrikesdepartementet samt finans- och justitieministerierna för att utreda brott mot ICT eller där man använt ICT.[136] Nederländernas nationella samordnare mot kontraterrorism (NCTb, National Coordinator for Counter

---

och Volendam år 2000 och 2001, terroristattacken den 11 september 2001, mordet på Pim Fortuyn år 2002 samt utbrottet av en smittsam fågelsjukdom år 2003 bidragit till denna utveckling.

[133] Regeringen stiftar lagar och förordningar, kvalitetssäkrar krishanteringskedjan, finansierar delar av den och genomför större satsningar inom området såsom gemensamma kommunikationssystem, varningssystem och erforderlig utrustning. Detta skiljer sig dock jmf. med den privata sektorn som tillhandahåller energi, finans tjänster, drickvatten, mat och sjukvård. Dessa sektorer ansvarar själva för tillgänglighet och integritet för produkterna och tjänsterna.

[134] Guus (Guusje) ter Horst är inrikesminister. Inom Inrikesdepartementet har generaldirektoratet för allmän ordning och säkerhet (Inspectie Openbare Orde en Veiligheid, DGV) ett övergripande ansvar för den holländska krisberedskapen. DGV är i sin tur uppdelat i fyra enheter; polis, brandkår och katastrofmedicin, kriskontroll och strategi. Idag samordnas krishanteringsarbetet av det ministerium som är mest berört av den aktuella krisen.

[135] Inrikesministern rapporterar om säkerhets- och krishanteringsarbetet till parlamentet minst vart fjärde år. Denna rapport baseras till stora delar på slutsatser från olika kommissioner, ordnings- och säkerhetsinspektionen och resultat från utredningar av händelser.

[136] The National High-Tech Crime Center

terrorism) har till uppgift att minimera risken för terrorattentat i Nederländerna samt vidta förebyggande åtgärder för att minska eventuella effekter tillföljd av ett terroristangrepp.[137] The Terrorism Warning System är ett av de verktyg som inrättats för att förbättra skydd av kritisk infrastruktur. Diskussioner förs kring huruvida systemet skulle kunna expanderas för att även inkludera andra typer av katastrofer.

År 2001 efterfrågade det nederländska parlamentet regeringen att dra upp en sektorsövergripande approach för skydd av kritisk infrastruktur. Man betonade särskilt vikten av att inte endast se på enskilda sektorer och infrastrukturer utan att man bör närma sig uppgiften utifrån ett övergripande, tvärsektoriellt och processorienterat perspektiv. Som en följd av detta initierades i april år 2002 ett projekt för skydd av kritisk infrastruktur (Project Bescherming Vitale Infrastruktur). Målet med projektet var att utveckla ett sammanhängande paket av åtgärder för att skydda kritisk infrastruktur i den offentliga och privata sektorn - välförankrat i den normala verksamheten.[138]

Projektets genomförande delades upp i olika faser. Under den första fasen gjordes med hjälp av ett Quick scan frågeformulär en inventering och identifiering av sektorer, produkter och tjänster som var att betrakta som nationell kritisk infrastruktur. I den andra fasen av programmet fick de olika sektorerna som identifierats ställa upp risk- och sårbarhetsanalyser. Då en stor del av den kritiska infrastrukturen ligger i händerna på privata aktörer skapades planerna i nära samverkan med den privata sektorn. Alla ministerier ansvarade för att utvärdera sina sektorers sårbarheter. Detta var första gången en analys av en sådan omfattning gjordes av den kritiska infrastrukturen i Nederländerna.[139]

I Nederländerna har 12 sektorer identifierats som kritiska. Respektive sektor har sedan, med utgångspunkt från tre kriterier, identifierat de produkter och tjänster (sammanlagt 33) som kan anses som nationellt kritiska. Totalt tog det ungefär tre år att identifiera den holländska nationella kritiska infrastrukturen.[140] Nedan ges en sammanställning över de identifierade CIP-sektorerna:

Tabell: Sammanställning över identifierade CIP-sektorer

Sektor	Vital produkt/tjänst	Ansvarigt departement
1. Energi	Elektricitet, naturgas, olja	Ministeriet för ekonomiska frågor
2. Telekommunikationer	Fast telefonkommunikation, mobil telekommunikation,	Ministeriet för ekonomiska frågor

[137] Organisatoriskt lyder NCTb under Justitiedepartementet och Inrikesdepartementet

[138] Det holländska nationella CIP-projektet hade tre övergripande målsättningar; (1) förebygga storskaliga avbrott eller störningar, (2) försäkra att de offentliga och privata sektorerna har tillräcklig beredskap för att hantera konsekvenserna av ett avbrott eller en störning och (3) medge att effektiva mildrande åtgärder tas för att förminska skada orsakad av avbrott eller störningar. Läs mer i "Policy letter on critical infrastructure protection to the Dutch parliament", [16:e september 2005]

[139] Luijf, Eric (2005)

[140] Vid den första inventeringen identifierades 11 kritiska sektorer och 31 kritiska produkter och tjänster. 2004 utökades denna lista till 12 sektorer och 33 kritiska produkter och tjänster. "Policy letter on critical infrastructure protection to the Dutch parliament", [16:e september 2005].

	radiokommunikation, navigering, satellit kommunikation, etermedier, Internet tillgång, post och kurirtjänst.	
3. Dricksvatten	Dricksvattentillgång	Ministeriet för hushållning, landanvändningsplanering och miljöledning.
4. Livsmedel	Livsmedelstillgång/livsmedelssäkerhet	Ministeriet för frågor om jordbruk, natur och livsmedelskvalitet.
5. Hälsa/Hälsovård	Olycksfall/annan sjukvård, medicin, serum och vaccin etc.	Ministeriet för hälsa, välfärd och sport.
6. Finansväsendet	Betalningsservice/betalningsstruktur	Finansdepartementet
7. Kontroll av kvalitet och kvantitet hos ytvatten	Vattenkvalitetsskötsel och kvantitet kontroll	Ministeriet för transport-, offentligt jobb- och vattenhållning
8. Allmän ordning och säkerhet	Upprätthållande av den allmänna ordningen och säkerheten	Inrikesdepartementet
9. Rättsordning	Administration av rättvisa och upprätthållande av lag och ordning	Justitiedepartementet
10. Offentlig administration	Diplomatisk kommunikation, information från regeringen, beväpnade styrkor, offentlig administration och beslutsfattande	Inrikesdepartementet
11. Transport	Huvudhamnen Schiphol och huvudhamnen Rotterdam, huvudvägar, vattenvägar, och huvudjärnvägar.	Ministeriet för transport-, offentligt jobb- och vattenhållning
12. Kemisk och nukleär industri	Transport, förvaring och produktion/förädling av kemiskt och nukleärt material.	Ministeriet för hushållning, landanvändningsplanering och miljöledning

Kommentar: Ingen inbördes rangordning gjordes utan samtliga ansågs ha passerat en viss kritisk tröskelnivå. Sektorerna är inbördes beroende av varandra då bortfall av en kritisk produkt eller tjänst inom en sektor kan få en dominoeffekt med stora konsekvenser för andra sektorer och för samhället som helhet.
Källa: Report on Critical Infrastructure Protection (16 september 2005)

Det holländska CIP-arbetet har beskrivits utförligt i rapporten ”Report on Critical Infrastructure Protection” som överlämnades till parlamentet den 16 september 2005.[141] Enligt rapporten användes tre övergripande kriterier för att identifiera kritiska infrastrukturer men det räckte med att ett av dessa kriterier var uppfyllt för att sektorn, tjänste- eller varuproduktionen skulle anses vara en kritisk infrastruktur;

1. Att ett bortfall eller en störning i en vital sektor, tjänste- eller varuproduktion medför stor ekonomisk eller social oro på nationell eller internationell nivå.

[141] Policy letter on critical infrastructure protection to the Dutch parliament, [16:e september 2005]

2. Att ett bortfall eller en svår störning resulterar direkt eller indirekt i ett stort antal offer.

3. Avsaknad av realistiska, färdiga och tillgängliga alternativ under återuppbyggnadstiden vid en långvarig störning.

Enligt rapporten har de olika sektorerna använt en steg-för-steg approach i analysarbetet och utgått ifrån tre huvudfrågor: (1) vilka är de kritiska produkterna, tjänsterna, processerna och sambanden?, (2) vad finns det för realistiska hot? och (3) är det nödvändigt att vidta ytterligare skyddsåtgärder? För att identifiera de realistiska hoten utarbetade sektorerna hotscenarier som baserades på tekniska förorsakanden och organisatoriska sammanbrott (inkl. oavsiktliga aktörsstyrda händelser) samt naturkatastrofer och avsiktliga aktörsstyrda händelser.

Efter identifieringen av landets kritiska produkter och tjänster förankrades dessa i respektive sektor för att därefter presenteras i en rapport till parlamentet. Utifrån konfidentiella sektorsvisa rapporter har man dragit slutsatsen att Nederländerna är ganska väl skyddat mot avbrott eller haveri i kritisk infrastruktur. Den övergripande planen för skyddet av landets kritiska infrastrukturer ska aktualiseras vart fjärde år.[142]

I det nationella arbetet med skydd av kritisk infrastruktur riktar man fokus mot beroenden mellan sektorer och fäster stor uppmärksamhet vid interaktionen med det regionala krishanteringssystemet då det är väldigt viktigt att försäkra sig om att säkerhetsplaner för den kritiska infrastrukturen är länkade med den lokala nivån och de lokala myndigheterna.[143]

Utöver den övergripande riskbedömningen som görs på nationell nivå försöker man också stimulera den privata industrin att göra egna riskbedömningar och analyser. I Nederländerna är drygt 90 % av den kritiska infrastrukturen privatägd och såväl den offentliga som den privata sektorn vidtar kontinuerligt åtgärder för att kunna garantera kontinuitet i den kritiska infrastrukturen. Utöver känslan av samhällsansvar uppges många företag ha tagit i beaktande de ekonomiska kostnader ett haveri i verksamheten skapar samt hur anseendet kan påverkas negativt och har därmed visat ett betydande egenintresse av att vidta åtgärder för att skydda den kritiska infrastrukturen.[144] Vad gäller finansiering av extra åtgärder för skydd av kritisk infrastruktur är varje sektor själv ansvarig för detta. Den offentliga sektorn ska bara täcka extra kostnader om staten bedömer att extra åtgärder måste vidtas och genomdriver detta genom bindande lagar eller liknande. Ersättning bestäms då från gång till gång.[145]

[142] Policy letter on critical infrastructure protection to the Dutch parliament, [16:e september 2005] samt presentations material WIB miniseminarium, Haag [26 april].
[143] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[144] Policy letter on critical infrastructure protection to the Dutch parliament [16 september 2005] samt intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007].
[145] Policy letter on critical infrastructure protection to the Dutch parliament [16 september 2005]

I Nederländerna strävar man efter att uppnå samarbete med den privata sektorn för att kunna skydda den kritiska infrastrukturen på bästa möjliga sätt.[146] För att bistå den privata sektorn i arbetet med att skydda den kritiska infrastrukturen har man etablerat ett nationellt rådgivningscentrum (NAVI) som gör det möjligt för ägare och operatörer i de kritiska sektorerna att utarbeta säkerhetsanalyser. Det nationella rådgivningscentret är inrättat för att stödja industrin och policyn är att endast stimulera, instruera och koordinera den privata sektorns egna säkerhetsarbete. NAVI etablerades i april 2007 och består för närvarande av 6 personer men kan eventuellt komma att behöva utökas i framtiden. För närvarande är NAVI ett experiment och totalt finansierat av staten men när man fattade beslut om att inrätta det nationella rådgivningscentret var målet att centret på några års sikt skulle kunna verka oberoende och finansiera sig självt. Det kan även i framtiden bli tal om någon form av finansiellt stöd från regeringen men på ett par års sikt är tanken att den service de tillhandahåller likaväl skulle kunna tillhandahållas kommersiellt och att centret självt ska kunna finansiera sin existens. Enligt representanter för det nederländska Inrikesdepartementet fanns det initialt en viss tveksamhet inför rådgivningscentret bland ägarna och operatörerna men denna tveksamhet uppges nu ha överkommits och fler och fler sektorer är villiga att delta genom att lägga fram frågor för diskussion och söka samarbete.[147]

Samråd med den privata industrin sker vidare inom ramen för the Strategical Assembly Vital Infrastructure, SOVI. SOVI utgör en grupp med personer på hög nivå från de olika sektorer som man arbetar med i projekt Vitaal. Gruppen fungerar som en plattform där representanter för de privata och offentliga sfärerna kan mötas för att diskutera CIP-frågor. SOVI består av en oberoende ordförande samt sektorsrepresentanter som koordinerar sin sektors röst. SOVI är tämligen oberoende och tar därmed ett eget ansvar för vilka frågor de vill driva och på vilket sätt. SOVI startade i september 2006 och möts ca 2-3 gånger per år. En av de största fördelarna med detta arrangemang anses vara att det medför att sektorerna blir bättre informerade om varandras behov och sårbarheter men också vilka andra sektorer som är beroende av ens egen funktionalitet. Tanken är vidare att s.k. besöksprogram för utvärdering av åtgärder för skydd av kritisk infrastruktur ska inrättas där representanter för de olika sektorerna ska besöka varandra. Målet är att detta ska bidra till att sektorerna får en uppfattning av hur nivån på skyddet av den kritiska infrastrukturen förhåller sig till ömsesidiga beroenden.[148]

I det nederländska arbetet med skydd av kritisk infrastruktur har framförallt tre brister identifierats. Det gäller dels oklarheter gällande den nödvändiga miniminivån för säkerhet för kritisk infrastruktur men också begränsningar i

[146] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[147] På sätt och vis kan man jämföra NAVI med förslaget om inrättandet av CIWIN då informationsdelning och utbyte av best practice i en säker miljö är en av NAVI:s funktioner. Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007].
[148] Policy letter on critical infrastructure protection to the Dutch parliament [16 september 2005]

tillgängligheten till kunskap och expertis på säkerhetsområdet. En annan brist som uppmärksammats var att det finns ett gap mellan hur privata och offentliga parter ställer sina säkerhetssatsningar till varandra.[149]

6.2 Inställning till direktivet för skydd av kritisk infrastruktur

Den nederländska regeringen intar en kritisk ståndpunkt till direktivförslaget om skydd av kritisk infrastruktur även om man övergripande stödjer målet med programmet och framhåller vikten av att skydda den kritiska infrastrukturen på bästa sätt. Den till viss del kritiska hållningen till direktivet handlar om att man vill värna subsidiaritetsprincipen och undvika dupliceringar av uppgifter och strukturer. Nederländerna argumenterar för att EPCIP endast bör binda medlemsstaterna till att påbörja eller vidareutveckla nationella CIP-program inom deras eget jurisdiktion.[150] Enligt Nederländerna ligger det främsta mervärdet i att ett direktiv kan bidra till en bättre kunskap om gränsöverskridande verkningar och att andra länder tar ett större ansvar för att skydda deras kritiska infrastruktur som många gånger kan få konsekvenser även för andra länder. Med hänvisning till detta mervärde uttrycker man samtidigt en oro över att man riskerar att inte nå det målet om direktivet blir för urvattnat.[151]

Många av artiklarna i direktivet är fortfarande under förhandling men i skrivande stund har Nederländerna lagt in reservationer mot artikel 2b som berör definitionen på ECI, samt artikel 5 och 6 som reglerar obligatoriet att upprätta säkerhetsplaner (OSP) och utpekandet av sambandsansvariga i säkerhetsfrågor (SLO).[152] Den holländska representanten säger sig dock inte tro att så många medlemsstater i slutändan kommer att ha några protester mot obligatoriet att inrätta säkerhetsplaner eller utse sambandsansvariga i säkerhetsfrågor utan att den huvudsakliga angelägenheten nu är själva definitionerna för utpekandet av ECI.[153] För att något ska utpekas som ECI framhåller Nederländerna att det bör beröra minst tre länder då den kritiska infrastrukturen som berör två länder kan lösas bilateralt. Vidare anser man att ett informationsutbyte kring skydd av kritisk infrastruktur bör ske i en miljö av tillit och konfidentialitet. CIWIN anser man endast bör utgöra ett instrument i att stärka utbytet av best practice, erfarenheter och kunskap utan att beröra utbyte av specifik information om hot eller underrättelser. Inställningen är vidare att ett kommittologiförfarande bör undvikas.[154]

[149] Policy letter on critical infrastructure protection to the Dutch parliament [16 september 2005]
[150] Nederländernas Non-paper (nr.2) (ej publicerat)
[151] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]. Som exempel nämner man bl.a. att många av attackerna på ICT-området kan härröra från andra länder.
[152] Tidigare var man också emot kommissionens förslag att lista europeisk kritisk infrastruktur men detta förslag har nu dragits tillbaka av kommissionen och upprättandet av listor är inte längre aktuellt. Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[153] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[154] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]

6.3 Bedömning av direktivets nationella konsekvenser

I Nederländerna har mycket gjorts kring skyddet av kritisk infrastruktur och detta är också något som man har framhållit i förhandlingarna runt direktivet genom att man ett flertal gånger har betonat att EPCIP bör ta hänsyn till vad som redan är organiserat nationellt, bilateralt och internationellt.

Då Nederländerna redan har en utarbetad nationell strategi för skydd av nationell kritisk infrastruktur är den holländska bedömningen att ett direktiv på det stora hela inte kommer att påverka deras nuvarande arbetssätt i någon större utsträckning. Man betonar här att det inte heller är tanken att direktivet ska vända upp och ner på det befintliga nationella systemen för hur man jobbar med skydd av kritisk infrastruktur utan snarare utgöra ett komplement till den nationella nivån. Man framhåller dock att många av skyldigheterna för ägarna och operatörerna av ECI måste skräddarsys per sektor vilket kommer att ta mycket tid och kraft i anspråk. Vad gäller de legala konsekvenserna av ett direktiv spekulerar man i att det i vissa sektorer kanske handlar om att en lag måste anpassas för att uppnå syftet och att det i andra fall kanske måste till ett tilläggsavtal.[155]

Vad gäller genomförandet av direktivet har Nederländerna i förhandlingarna förespråkat en frivillig approach snarare än ett obligatorium och tvingande lagstiftning. Tjänstemannen på det nederländska Inrikesdepartementet framhöll under intervjun att kommissionen betonat att bindande lagstiftning visserligen inte kan uteslutas men att det inte heller nödvändigtvis behöver vara så, men att när man sedan lät nationella rättsexperter granska hur artiklarna var formulerade så hävdar de att lagstiftning måste till och att överenskommelser inte alls skulle räcka.[156] I Nederländerna har man därför tillsatt en juridisk arbetsgrupp för att undersöka de legala konsekvenserna av direktivet. Arbetsgruppen har kommit med ett första rådgivande utkast men den slutliga rapporten är inte offentlig än då den till viss del också berör de pågående EPCIP-förhandlingarna.[157]

Givet att de sektoriella kriterierna ännu inte är fastslagna och att procedurstegen inte har bestämts vill man från holländskt håll inte kommentera antalet potentiella ECI eller ge exempel på vad som skulle kunna tänkas bli utpekat som ECI i landet. Man framhåller dock att det nuvarande direktivförslaget föreslår att det ska vara upp till varje medlemsstat att godkänna ett utpekande av en ECI inom landets territorium och att det därmed finns ganska många utvägar.[158]

I Nederländerna är det ägarna och operatörerna av kritisk infrastruktur som ansvarar för att vidta åtgärder för att göra dem säkrare och alla kostnader måste bäras av industrierna själva. Den holländska regeringen stödjer dem inte finansiellt men kan indirekt bistå med rådgivning och vägledning via det

[155] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[156] Man uppger att det t.ex. gäller formuleringar som ”member states shall ensure..”. Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[157] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[158] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]

nationella rådgivningscentret för kritisk infrastruktur (NAVI).[159] Vad gäller inrättandet av Operator Security Plans (OSP) är de flesta ägare och operatörer redan förpliktade att inrätta något liknande de säkerhetsplaner som föreslås i direktivet inom ramen för respektive sektors säkerhetsföreskrifter. I Nederländerna har man listat tolv kritiska sektorer men det finns ingen generell lagstiftning om att alla dessa ska upprätta säkerhetsplaner utan detta varierar från sektor till sektor.[160]

Samma slutsats dras vad gäller sambandsansvariga i säkerhetsfrågor (SLO) där intervjupersonen bedömer att många stora företag redan har en Chief Executive Officer (CEO) inom styrelsen som är ansvarig för säkerhetsfrågor. Den holländska inställningen är att så snart man vet vad som kommer att bli utpekat som ECI i landet så kommer man också att veta vilka som ska utses som SLO. Den nederländska representanten bedömer att det i de flesta fall kommer att bli den styrelsemedlem som redan idag är ansvarig för säkerhetsfrågor.

I dagsläget innehar en person inom det nederländska Inrikesdepartementet rollen som nationell kontaktpunkt för CIP-frågor och enligt uppgifter avser man inte att utse någon ny myndighet till följd av ett direktiv på området utan funktionen kommer även i fortsättningen att bedrivas i Inrikesdepartementets regi.[161]

De budgetära konsekvenserna av ett eventuellt direktiv på området har ännu inte bedömts men mot bakgrund av att många ägare/operatörer redan har något motsvarande de säkerhetsplaner och sambandsansvariga i säkerhetsfrågor som direktivets artikel 5 och 6 stipulerar bedöms kostnaderna inte bli särskilt omfattande. Den övergripande nederländska bedömningen är således att en implementering av ett eventuellt direktiv mer kommer att handla om en legislativ börda än en budgetär sådan.[162]

6.4 Sammanfattning

Den holländska regeringen uppger att man övergripande stödjer målet med det europeiska programmet för skydd av kritisk infrastruktur. Den till viss del kritiska hållningen till direktivet handlar om att man vill värna subsidiaritetsprincipen och undvika dupliceringar av uppgifter och strukturer. Det direkta mervärdet som framhålls är i holländsk mening framförallt att programmet leder till en bättre insikt i gränsöverskridande verkningar och att direktivet kan bidra till att andra länder tar ett större ansvar för att skydda deras kritiska infrastruktur som många gånger kan få konsekvenser även för andra länder. Den holländska bedömningen är att

[159] Det kan bl.a. handla om att tillhandahålla stöd för att göra analyser men också att ge information anpassad till sektorerna så att de kan arbeta fram säkerhetsplaner samt bli informerade om relevanta hot. Om den nederländska underrättelsetjänsten t.ex. får information från USA om att det finns ett hot mot kemiska anläggningar kommer denna information att spridas inom NAVI och dess säkra informationsdelningssystem så att ägarna och operatörerna av exempelvis kemiska fabriker vet att detta hot existerar och kan vidta åtgärder för att hindra detta från att ske. Det handlar enbart om information i förebyggande syfte inte kommunikation om vad som händer när något verkligen går snett.
[160] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[161] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]
[162] Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]

direktivet inte kommer att påverka det nationella arbetet på området i någon större utsträckning. Givet att många av ägarna och operatörerna redan har något liknande de säkerhetsplaner och sambandsansvariga i säkerhetsfrågor som direktivet föreskriver är den övergripande nederländska bedömningen att en implementering av direktivet mer kommer att handla om en legislativ börda än en budgetär sådan. Mot bakgrund av denna bedömning har man i Nederländerna tillsatt en juridisk arbetsgrupp för att undersöka de legala konsekvenserna av direktivet. Arbetsgruppen har utkommit med en preliminär bedömning av direktivets legala konsekvenser men denna rapport är inte offentlig.

7 STORBRITANNIEN

I nedan sektion ges en översiktlig beskrivning av det brittiska arbetet med skydd av kritisk infrastruktur med fokus på vad man definierar som kritisk infrastruktur, hur ansvars- och ledningsstrukturer ser ut, vilken roll de lokala myndigheterna, departementen och andra centrala aktörer har samt hur CIP-åtgärder finansieras. Avsnittet avslutas med en sammanfattning av den brittiska synen på EPCIP och vilka förberedelser som har vidtagits för en eventuell implementering av ett direktiv.

Förkortningar

CCS	The Civil Contingencies Secretariat
CERT	Computer Emergency Response Team
CPNI	Centre for the Protection of National Infrastructure
CNI	Critical National Infrastructure
CSIA	The Central Sponsor for Information Assurance
DSTL	The Defence Research Centre
IAAC	The Information Assurance Advisory Council
LGD	Lead Government Department
MoD	The Ministry of Defence
NHTCU	The National High Tech Crime Unit
NISCC	National Infrastructure Security Co-ordination Centre (har numera integrerats i CPNI)
NSAC	The Security Service's National Security Advice Centre

7.1 Landets arbete med skydd av kritisk infrastruktur

I Storbritannien uppfattas skyddet av den kritiska infrastrukturen som en väsentlig del av krisberedskapen. Det begrepp som används är "Critical National Infrastructure" (CNI)[163] vilket definieras som:

> ...those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could: (1) cause large scale loss of life, (2) have a serious impact on the national economy, (3) have other grave social consequences

[163] Termen nationell har lagts till för att förtydliga att listan över kritisk infrastruktur endast innefattar den infrastruktur som är kritisk med hänsyn till det brittiska nationella intresset.

> for the community or (4) be of immediate concern to the government.[164]

Det brittiska nationella CIP-programmet har pågått i drygt fyra år i dess nuvarande form även om aktiviteter och nationella initiativ har utvecklats sedan 1980-talet i samband med IRA-terrorismen uppkomst.[165] I Storbritannien har man identifierat nio sektorer som tillhandhåller samhällsviktiga tjänster och inom dessa sektorer har man sedan pekat ut nyckelelement som nödvändig samhällsservice inte kan levereras utan och som därmed utgör nationell kritisk infrastruktur (dessa komponenter kan vara såväl materiella som elektroniska).[166]

Tabell: Sammanställning över sektorer som betecknas som nationell kritisk infrastruktur (CNI)

Sektor	Delsektorer	Ansvarigt departement
1) Kommunikationer	Datakommunikationer, fast kommunikation, e-post, offentlig information, trådlös kommunikation	• Department for business, enterprise and regulatory reform (BERR)
2) Räddningstjänst	Ambulans, brandkår, marin, polis	• Department of Health (DH) • Communities and local government (CLG) • Department for Transport (DfT) • Home Office
3) Energi	Elektricitet, naturgas, råolja	• Department for business, enterprise and regulatory reform (BERR)
4) Finansväsendet	Kapitalförvaltning, investment banking, marknader, bankverksamhet	• HM Treasury (HTM)
5) Livsmedel	Producering, importering, process, distribution, detaljhandelsförsäljning	• Department for the Environment, Food and Rural Affairs (DEFRA) • Food Standards Agency (FSA)
6) Regering och statsmakt	Central förvaltning, regional förvaltning, lokal förvaltning, parlament och lagstiftning, rättvisa, nationell säkerhet	• Cabinet Office (CO)
7) Hälsa	Hälsa, hälsovård	• Department of Health (DH)
8) Transport	Flyg, marin, järnvägar, vägar	• Department for Transport (DfT)
9) Vatten	Vatten, avlopp	• Department for the Environment, Food and Rural Affairs (DEFRA)

Kommentar: Denna lista används av alla brittiska myndigheter som är involverade i CIP, CIIP eller krisberedskap. Då många av aktörerna som idag tillhandahåller den samhällsviktiga verksamheten är privata har den brittiska staten ett nära samarbete med de organisationer och företag som tillhandahåller dessa tjänster så att de är skyddade i proportion till de eventuella hot som kan existera. The Security Service ansvarar för identifieringen av nationell kritisk infrastruktur i samarbete med relevanta ministerier och deras sektorsorganisationer. Definitionerna och den strategiska approachen ses över regelbundet. För drygt ett år sedan minskade man listan från 10 sektorer till 9 (sektorn som togs bort var ”public safety”).

[164] Punktsatserna uttrycker de konsekvenskriterier som används för att identifiera en kritisk infrastruktur (CNI). Centre for the Protection of National Infrastructure (CPNI)
[165] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[166] Centre for the Protection of National Infrastructure (CPNI)

Källa: Centre for the Protection of National Infrastructure (CPNI)

Likt USA står Storbritannien inför hot om terroristattacker och skyddet av den nationella kritiska infrastrukturen är därför en viktig del i kampen mot terrorism.[167] Sektorer som energi, transport och finanssystem uppges vara särskilt utsatta för denna typ av hot och mot denna bakgrund avser den brittiska staten att särskilt prioritera skyddet av nationell kritisk infrastruktur mot terroristattacker på installationer och utrustning samt elektroniska attacker riktade mot datorer och kommunikationssystem.[168]

Storbritannien har mycket stora ministerier med en förvaltningsstruktur som bygger på principen om ministerstyre, dvs. att enskilda ministrar har ett direkt ansvar för genomförandet av politiken. Som en naturlig följd har ministrar därför ett intresse av att ha direkt kontroll över den underlydande förvaltningens verksamhet och krishanteringsfrågor stannar därför vanligtvis inom ministerierna.[169] I Storbritannien ansvarar Inrikesdepartementet för koordineringen av CIP-frågor. Likt krisberedskapsarbetet i stort gäller dock att även om det övergripande koordineringsansvaret för skydd av kritisk infrastruktur ligger under inrikesministern så är även andra departement involverade i skyddet av de olika identifierade sektorerna. Respektive ministerium har exempelvis ett övergripande ansvar att säkerställa att nödvändiga åtgärder tas inom deras sektor. Departementen leder likaså identifieringen av den kritiska infrastrukturen inom sina respektive sektorer i samråd med centret för skydd av nationell infrastruktur (CPNI) och andra sektorsorganisationer.[170]

Som ovan nämndes är en av de främsta tillhandahållarna av säkerhetsråd kring den brittiska nationella kritiska infrastrukturen the Centre for the Protection of National Infrastructure, CPNI.[171] CPNI är en statlig myndighet vars uppgift är att tillhandahålla integrerade säkerhetsråd kring nationell kritisk infrastruktur till företag och organisationer. CPNI svarar inför generaldirektören på MI5 och verkar under the Security Service Act 1989.[172] Även The National High Tech Crime Unit (NHTCU) som sedan april 2007 har blivit en integrerad del av the Serious Organised Crime Agency (SOCA) och säkerhetspolisen arbetar nära CPNI genom att bidra med sin expertis vid kartläggningar av hot, underrättelser och säkerhet. En annan viktig aktör inblandad i skyddet av den brittiska nationella kritiska infrastrukturen är The Central Sponsor for Information Assurance (CSIA) som bildades som en del av premiärministerkansliet den 1 april 2003. CSIA ansvarar för CIIP som enbart fokuserar på CNI och är också en del i den bredare informationssäkerhetsstrategin. IAAC står för The Information Assurance

[167] Se Storbritanniens counter terrorism strategy, CONTEST
[168] Centre for the Protection of National Infrastructure (CPNI)
[169] Centre for the Protection of National Infrastructure (CPNI)
[170] Centre for the Protection of National Infrastructure (CPNI)
[171] CPNI bildades i februari 2007 genom en sammanslagning av the National Infrastructure Security Co-ordination Centre (NISCC), en del av den brittiska säkerhetstjänsten (MI5) och the National Security Advice Centre (NSAC). Källa: The British security service (MI5)
[172] Källa: The British security service (MI5). Dessa inkluderar bl.a. MI5, CESG (Communications Electronics Security Group), the UK's National Technical Authority for Information Assurance och andra departement ansvariga för nationell kritisk infrastruktur inom sina respektive sektorer.

Advisory Council och är en annan nyckelaktör inblandad i just skydd av kritisk infrastruktur. IAAC bildades år 2000 och är ett privatsektorsorgan som speciellt arbetar för att utveckla informationssäkerheten. I IAAC sitter regeringen med som representant men organet är inte organisatoriskt en del av regeringen. IAAC har sammanlagt fem arbetsgrupper som jobbar inom områden kopplade till informationssäkerhet. IAAC är en kanal för privatoffentlig samverkan och ska som sådan bl.a. underlätta dialog och utbyte av information kring just informationssäkerhet.[173]

7.2 Inställning till direktivet för skydd av kritisk infrastruktur

När Storbritannien lämnade kommentarer på kommissionens grönbok 2005 rörde synpunkterna framförallt vad som ska betraktas som ECI, ansvarsfrågor, koppling till riskanalyser och antiterrorismarbetet samt definitioner. En jämförelse ger vid handen att britterna inte var några starka förespråkare för behovet av ett direktiv då och inte heller är det nu. I dagsläget är det framförallt tre punkter som britterna framhåller som problematiska. Det handlar först och främst om definitionen av ECI vilken man anser är för bred. Den andra tveksamheten rör obligatoriet kring inrättandet av OSP och SLO. Från brittiskt håll anser man att det är principiellt felaktigt att inrättandet av OSP och SLO överhuvudtaget föreslås utan någon som helst föreliggande analys där man kommit fram till att det finns ett problem som man måste komma tillrätta med genom att just lagstifta om upprättande av säkerhetsplaner och sambandsansvariga i säkerhetsfrågor. Enligt den brittiska uppfattningen skulle det ha varit bättre att först göra en behovsanalys och sedan, utifrån behovsanalysen, fastslå vad som måste göras. Den tredje invändningen rör säkerhetsaspekterna av att på något sätt lista ECI. Direktivet är visserligen mycket bättre på denna punkt nu jämfört med tidigare men man är från brittiskt håll fortfarande inte helt övertygade om att problemet är helt ur världen. Britternas generella ståndpunkt är att skydd av kritisk infrastruktur främst är ett nationellt ansvar och att värdet av ”European efforts” på området, i relation till de kostnader och risker som det medför, är ganska låga. Mot denna bakgrund och efter känningar om att ett direktiv inte går att undvika har den brittiska strategin varit att försöka mildra direktivförslagets obligatoriska inslag i så pass hög grad som möjligt.[174] Enligt den brittiske representanten kommer Storbritannien trots allt att stödja inrättandet av ett direktiv så länge det inte leder till en identifiering och förteckning över ECI. Från brittiskt håll framhålls att det är svårt att förespråka något annat eller stoppa ett direktiv pga. frågans karaktär - man kan helt enkelt inte argumentera emot själva grundtanken att förbättra skyddet för europeiskt kritisk infrastruktur. Britterna förväntar sig se ett direktiv implementeras någon gång under årets lopp. I sammanhanget nämndes att fransmännen innehar ordförandeskapet till hösten 2008 och att de troligtvis är angelägna över att få driva igenom ett direktiv på området då programmet är väldigt likt det sätt fransmännen redan jobbar på nationellt. Enligt den brittiska representanten har många länder idag aktivitet utspridd på olika sektorer men de har ofta inte gjort

[173] The Information Assurance Advisory Council (IAAC)
[174] Mötesanteckningar ProCiv hösten 2007

någon fullständig sektorsöverskridande analys och saknar dessutom en sektorsöverskridande funktion. Vid intervjun framkom att man därför tror att många medlemsstater sätter sin tilltro till direktivet och tänker använda det för att få igång ett eget nationellt CIP-program samt få till stånd en välfungerande koordinering mellan de olika sektorerna.[175]

7.3 Bedömning av direktivets nationella konsekvenser

I Storbritannien har man inte föreslagit eller vidtagit några särskilda åtgärder för att förbereda för en eventuell implementering av ett direktiv. Dock har man gjort en analys av vad direktivet förväntas få för konsekvenser nationellt. Inom ramen för konsekvensanalysen tittade man på vad som redan görs nationellt, hur man skulle kunna genomföra direktivet och vilka konsekvenser det eventuellt skulle kunna få. Utöver det har man också haft ett flertal workshops och möten med de departement som kommer att beröras av direktivet.

Britterna har även gjort en preliminär uppskattning av vad som eventuellt skulle kunna bli utpekat som ECI i landet. Bedömningen är att det kan komma att handla om drygt 10 stycken utpekade ECI nationellt men man betonar att detta endast är en preliminär uppskattning och att det i slutändan beror på hur bred definitionen blir. Exempel på vad som bedömdes kunna bli utpekat som ECI var exempelvis London som finansiellt centrum, energitillförsel/förråd med Irland samt energilänkar ner till Nederländerna och Belgien. Som direktivförslaget ser ut nu skulle även saker på den nukleära sidan kunna bli utpekat som ECI pga. den miljöpåverkan dessa har. Den brittiska inställningen är dock att ett direktiv som omfattar denna sektor inte kommer att tillföra något då kärnkraftsanläggningar redan är några av de bäst skyddade kritiska infrastrukturerna genom andra lagar och förordningar. Inget skulle med andra ord förändras genom att dessa också utpekas som europeisk kritisk infrastruktur. Efter den slutliga definitionen hoppas man från brittiskt håll att man inom hela EU totalt inte ska identifiera mer än drygt 100 ECI. Det är också därför man nu arbetar hårt på att få till en passande definition.[176]

Vid snabbanalysen av vad en implementering av ett direktiv på området skulle kunna innebära gjordes också en beräkning av kostnaderna kopplade till detta genom att man från varje område samlade in information om de uppskattade merkostnaderna.[177] Efter en uppskattning av potentiella ECI i landet granskades dessa mer i detalj och en övergripande slutsats var att allt som man förväntade sig skulle kunna bli utpekat som ECI redan hade en säkerhetsplan samt en sambandsansvarig i säkerhetsfrågor motsvarande det som direktivet stipulerar. I de flesta fall är dessa frivilliga arrangemang eller reglerat i sektorslagstiftning och det finns således ingen generell

[175] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[176] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[177] Denna konsekvensstudie är inte offentlig men uppgavs vara väldigt ungefärlig och generell till sin karaktär. Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

lagstiftning som tvingar ägare och operatörer av nationell kritisk infrastruktur att inrätta varken OSP eller SLO.[178]

I Storbritannien åligger det säkerhetskoordineraren på myndigheten eller företaget att ta fram en säkerhetsplan. I stora organisationer rekommenderas att denna roll ligger på styrelsenivå och i mindre organisationer bör ansvaret åtminstone ligga på seniornivå. Till säkerhetskoordinerarens huvuduppgifter hör (1) att ansvara för skapandet av en säkerhetsplan baserat på en hot- och risk bedömning, (2) att säkerställa att säkerhetsåtgärder är genomförda och testade, (3) att bestämma när anläggningar åter kan tas i bruk efter att de blivit evakuerade samt att (4) samverka med polis, annan räddningstjänst och lokala myndigheter. Till säkerhetskoordinerarens uppgifter hör också att (5) anordna personalövningar samt (6) utföra regelbundna inspektioner av säkerhetsåtgärder och procedurer.[179] Säkerhetsplanen bör innehålla detaljer kring alla förebyggande säkerhetsåtgärder som ska genomföras, instruktioner kring hur man ska svara på ett hot, instruktioner för hur man ska agera vid ett misstäkt föremål eller händelse, en ”search plan”, en evakueringsplan, en plan för att säkerställa verksamhetens kontinuitet samt en kommunikations- och mediastrategi för att hantera förfrågningar från allmänhet och oroliga anhöriga.[180]

Vad gäller kravet om att genomföra hot och riskbedömningar så gör man redan nu regelbundna bedömningar av hot och risker inom respektive sektor och man har också en generell hot- och riskbedömning som man jobbar efter. Med beaktande av det som redan görs på nationell nivå på denna punkt kommer m a o kravet om upprättandet av säkerhetsplaner att vara en del av något som redan görs av the security service och departementen i samråd med ägarna/operatörerna.[181]

I Storbritannien har alla ägare/operatörer av nationell kritisk infrastruktur, uppemot 1000 i hela landet, fri tillgång till s.k. ”security advisers”. Dessa rådgivare upplyser bl.a. kring olika säkerhetsåtgärder som man borde anta, lämpliga kvalifikationer för den som är säkerhetsansvarig samt behovet av säkerhetsplaner och kontinuitetsplaner. Allt är dock att betrakta som råd och är inte tvingande på något sätt. Den brittiska erfarenheten är dock att råden generellt brukar tas i beaktande och man har gjort bedömningen att en frivillig approach gentemot operatörerna är det mest effektiva.

Då översynen av säkerhetsarbetet kring all potentiell ECI inom landet visade att något motsvarande OSP och SLO redan var väletablerat hos de potentiella ECI-ägarna och operatörerna i Storbritannien gjordes bedömningen att en implementering av direktivet inte skulle innebära några extra kostnader. Det framhölls dock att ett direktiv på området indirekt kan innebära en merkostnad för ägarna och operatörerna i och med att dessa kan behöva säkerställa att de följer eventuell ny lagstiftning. Det gjordes

[178] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[179] Centre for the protection of national infrastructure (CPNI)
[180] Centre for the protection of national infrastructure (CPNI)
[181] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

dock ingen uppskattning av hur mycket pengar det kan röra sig om i detta fall.[182]

Vad gäller rollen som kontaktpunkt i CIP-frågor har man i Storbritannien flera kontaktpunkter för CIP-frågor runtom på de olika departementen även om Inrikesdepartementet har den koordinerande rollen. Vid en eventuell implementering av direktivet avser man i dagsläget inte att utse någon ny CIP Contact Point utan denna funktion kommer även fortsättningsvis att ligga inom Inrikesdepartementet. Om det däremot visar sig att funktionen då direktivet är färdigförhandlat blir mer teknisk till sin karaktär så kan dock kontaktpunkten komma att flytta över till CPNI eftersom det är dem som har alla rådgivare, kontakter till folk runt om i landet samt sitter på den tekniska kompetensen. Under den närmaste framtiden så kommer denna roll dock fortsatt ligga på Inrikesdepartementet.[183]

Den samlade brittiska bedömningen är att införandet av lagstiftning kommer att vara den största konsekvensen för deras nationella system för skydd av kritisk infrastruktur. En högst snabb och preliminär uppskattning är att det skulle kosta uppemot 10 miljoner euro att implementera lagstiftningskravet.[184] Den brittiska uppfattningen är dock att man i dagsläget redan har ett välfungerande frivilligt arrangemang med ägare och operatörer som litar på statens råd och man hyser därför stor oro för att lagstiftning på området skulle medföra förändringar i förhållandet till operatörerna som i värsta fall kan riskera att få motsatt effekt.[185]

7.4 Sammanfattning

Storbritanniens synpunkter på kommissionens grönbok om ett europeiskt program för skydd av kritisk infrastruktur (EPCIP) 2005 rörde framförallt vad som var att betrakta som europeisk kritisk infrastruktur, ansvarsfrågor, koppling till riskanalyser och antiterrorismarbetet samt definitioner. Storbritanniens synpunkter skiljde sig inte nämnvärt från vad Sverige framförde och synpunkterna på grönboken stämmer fortfarande väl in på den brittiska officiella linjen. Britterna är inga starka förespråkare för behovet av ett direktiv på området och i dagsläget är det framförallt obligatoriet kopplat till artiklarna 5 och 6 som man anser är problematiska. Som en följd av detta och efter känningar om att ett direktiv inte går att undvika har den brittiska strategin i EU-förhandlingarna varit att försöka mildra direktivet i så pass hög grad som möjligt.[186] Den brittiska inställningen är att direktivet inte kommer att tillföra något avgörande för

[182] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[183] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[184] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[185] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[186] Också Sverige, Nederländerna och Danmark har deltagit i arbetet med att mjuka upp direktivet för att få till stånd ett mer flexibelt instrument. Detta arbete har också gett utdelning då det lett till kompromisser med kommissionen vad gäller t.ex. listning av europeisk kritisk infrastruktur (ECI) samt utformningen av Operator Security Plans och Security Liaison Officers. Jmf. Förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna. [KOMMISSIONEN (2006) 787]. Den senaste versionen från kommissionen är daterad 19 februari 2008 (5051/2/08 – REV 2).

deras nuvarande arbete på området, men genom att mildra direktivet kommer man inte heller att förlora på det. I sammanhanget framhåller man visserligen argumentet om att det finns andra medlemsländer vars skydd av kritisk infrastruktur fortfarande är mycket outvecklad och att ett europeiskt program kan hjälpa andra medlemsstater att förbättra sig på området vilket i förlängningen skulle vara till nytta för alla medlemsstater men man anser trots allt inte att det finns något värde av att alla måste följa samma approach då man inte har samma förutsättningar och inte står inför samma hot. Enligt den brittiska hållningen skulle ett utbyte av best practice, som är frivilligt för medlemsstater att anta och följa om de så väljer, räcka.[187]

Den brittiska bedömningen är att införande av lagstiftning kommer att bli den främsta konsekvensen på nationell nivå. Den brittiska oron för ett direktiv på området grundar sig i att man befarar att lagstiftningstvånget kan skapa problem i relationen till ägarna och operatörerna av den utpekade europeiska kritiska infrastrukturen och därigenom äventyra det förtroendet som har byggts upp.[188]

[187] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]
[188] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

8 SAMMANFATTANDE ANALYS

Sveriges medlemskap i EU innebär att vi på olika sätt påverkas av utvecklingen inom unionen. En viktig fråga på krisberedskapsområdet som kommer att påverka det svenska krishanteringssystemet framöver är det europeiska programmet för skydd av kritisk infrastruktur (EPCIP). Programmet föreslås bestå av tre huvuddelar; ett direktiv, ett finansieringsprogram samt ett informations- och varningssystem (CIWIN).

När utvecklingen på krisberedskapsområdet går mot allt mer samarbete och samverkan utanför den nationella arenan är det viktigt att vi tar del av goda exempel som kan bidra till att utveckla det nationella krishanteringssystemet. Ett sätt att förbereda oss på vad som komma skall är att blicka ut mot andra EU-länder för att se hur dessa arbetar med skydd av kritisk infrastruktur och vad de bedömer att ett direktiv skulle kunna få för nationella konsekvenser på området. I detta kapitel jämförs Danmarks, Finlands, Nederländernas och Storbritanniens inställning till direktivet, vilka konsekvenser de bedömer att ett direktiv skulle få på den nationella nivån samt vilka förberedelser som vidtagits för en eventuell implementering av ett direktiv.

En kort sammanfattning av de bindande artiklarna i direktivet ger vid handen att en implementering av direktivet kommer att erfordra ett omfattande identifieringsarbete av potentiell europeisk kritisk infrastruktur (ECI), såväl inom som utanför det egna landets gränser. Efter denna identifiering kommer ägare och förvaltare av en utpekad ECI åläggas att upprätta en säkerhetsplan för den kritiska anläggningen (en s.k. Operator Security Plan, OSP) samt utse en sambandsansvarig i säkerhetsfrågor (en s.k. Security Liaison Officer, SLO). Säkerhetsplanen ska följa en standardiserad europeisk modell och bland annat omfatta vilka anläggningar som är kritiska samt vad som görs för att skydda dem såväl permanent som vid en kris. 24 månader efter utpekandet av en ECI ska kommissionen informeras om läget sektorsvis. Varje medlemsstat ska vidare utse en kontaktpunkt för skydd av europeisk kritisk infrastruktur (en s.k. CIP Contact Point) som ska koordinera arbetet i landet samt gentemot andra medlemsländer och kommissionen.

Såväl Nederländerna som Storbritannien och Finland inledde sitt arbete med skydd av kritisk infrastruktur under slutet av 1990-talet och i samtliga av dessa länder har reformer på området påskyndats av händelserna i USA den 11 september 2001 och den förstärkning av terrorhotet som följt i dess spår. En studie av det nationella arbetet på området ger vid handen att man i många av de undersökta länderna arbetar på ett delvis likartat sätt med CIP-frågor. I samtliga länder är det övergripande skyddet för den kritiska infrastrukturen uppdelat på respektive ministerium. Som en följd av denna uppdelning har man också fäst stor uppmärksamhet på att tillgodose det ökade behovet av samordning och inte sällan inrättat centrala regeringsorgan för att stödja samordningen mellan departement, myndigheter och områdesansvariga aktörer. Då en stor del av den kritiska infrastrukturen ligger i händerna på privata ägare och operatörer har man i

flera av länderna också genomförts olika slags koordineringsaktiviteter mellan den offentliga sektorn och näringslivet. I Finland har exempelvis Försörjningsberedskapscentralen (FBC) kontinuerliga kontakter med den privata sektorn och hjälper aktörerna att upprätta säkerhetsplaner samt att göra risk- och sårbarhetsanalyser och i Nederländerna erbjuds en liknande hjälp inom ramen för det nyinrättade nationella rådgivningscentret för skydd av kritisk infrastruktur, NAVI.[189] I Storbritannien har the Centre for the Protection of National Infrastructure (CPNI) motsvarande funktion och landets drygt 1000 ägare och operatörer av kritisk infrastruktur har fri tillgång till s.k. ”security advisers” som bl.a. lämnar upplysningar om olika säkerhetsåtgärder som bör antas, lämpliga kvalifikationer för den som är säkerhetsansvarig, bedömningar om behovet av säkerhetsplaner etc. Trots att detta inte är något som är tvingande i något av länderna utan snarare ska betraktas som goda råd är bl.a. den brittiska erfarenheten att det privata näringslivet generellt brukar ta råden i beaktande.

Nedanstående tabell presenterar en översikt över de nationella systemen för skydd av kritisk infrastruktur.

Tabell: Översikt av de nationella systemen för skydd av kritisk infrastruktur

Land / Jämförelsepunkt	Danmark	Finland	Nederländerna	Storbritannien
När började man arbeta med CIP?	-	1995	1999	1999
Nationell CIP-strategi?	-	Ja	Ja	Ja
Approach på strategin	-	All hazards → CIIP	CIIP → All hazards	All hazards → CIIP
Perspektiv	-	Systemperspektiv	Systemperspektiv	Systemperspektiv
Har CI-sektorer identifierats?	-	Ja	Ja	Ja
Har CI-undersektorer identifierats?	-	Ja	Ja	Ja
Finansiering av CIP-åtgärder	-	Ägare/operatörer ansvarar för skyddet av de egna anläggningarna men staten kan medfinansiera indirekt.	Ägare/operatörer ansvarar för skyddet av de egna anläggningarna men staten kan medfinansiera i särskilda fall.	Ägare/operatörer ansvarar för skyddet av de egna anläggningarna
Centrala aktörer	• Försvarsmin. • BRS • PET	• Inrikesmin. • FBC + FEP • FICORA	• Inrikesmin. (NCC, ERC, AIVD, NHTCC, NCTb)	• Inrikesmin. (CPNI, CCS, CSIA)

[189] Nationaal Adviescentrum Vitale Infrastructuur

	• FE			• SOCA
Privat-offentlig samverkan (PoS)	• BRS	• FBC (NESA) • FEP (NBED) • ACIS • VAHTI	• SOVI (strategisk) • NAVI (operativ)	• CPNI • IAAC

Kommentar: Sammanställningen är inte heltäckande. Förklaringar till förkortningarna hittas under respektive landgenomgång.

Vad gäller inställningen till ett direktiv för skydd av kritisk infrastruktur är en slutsats man kan dra att samtliga av de granskade länderna övergripande stödjer målet med programmet och framhåller vikten av att skydda kritisk infrastruktur på bästa sätt. Lite hårddraget kan man säga att länderna i studien delar upp sig i två läger där Nederländerna, Danmark och Storbritannien har stått nära varandra i förhandlingarna emot ett direktiv medan Finland å andra sidan tenderar att för det mesta sluta upp bland förespråkarna för ett direktiv. Den till viss del kritiska hållningen till direktivet som bland annat kan skönjas hos Danmark, Nederländerna och Storbritannien handlar om att man vill värna subsidiaritetsprincipen och undvika dupliceringar av uppgifter och strukturer. Sett till de bindande artiklarna i direktivet det framförallt artiklarna 5 och 6 som reglerar obligatoriet att upprätta säkerhetsplaner och utpeka sambandsansvariga i säkerhetsfrågor som är problematiska.[190] Från finskt håll betonas å andra sidan att även om man har kommit olika långt i olika länder och vidtagit varierande åtgärder så måste infrastrukturägarna generellt höja säkerheten och man anser att det behövs en bindande lag för att uppnå detta. I dagsläget är inga artiklar problematiska för Finland och generellt är man från finskt håll också ganska nöjda med innehållet i det nu liggande direktivet.

Enligt medlemsstaterna i denna studie är det direkta mervärdet med ett direktiv framförallt att det kan leda till bättre kunskaper om gränsöverskridande verkningar samt att direktivet kan bidra till att länder tar ett större ansvar för att skydda deras kritiska infrastruktur vilken många gånger kan få konsekvenser även för andra länder. Från bl.a. brittiskt håll bedömer man vidare att många länder troligen ser ett EU-direktiv som en chans att ta kontroll över den kritiska infrastrukturen i sina länder som till stora delar ligger i händerna på privata aktörer.[191] Finländarna betonade att ett av de främsta mervärdena med en EU-ram på området är att det medför att konkurrensen på marknaden inte störs. Då åtgärder för att skydda den kritiska infrastrukturen ofta leder till direkta ekonomiska merkostnader anser man från finskt håll att dessa också ska vara lika för alla infrastrukturägare i alla länder. Om grunderna för identifieringen och klassificeringen av objekt inom den kritiska infrastrukturen på EU-nivå stärks genom en bindande rättsakt garanteras med andra ord ett jämlikt och enhetligt förhållningssätt och förfarande medlemsländerna emellan men

[190] Alla tre länderna har exempelvis under förhandlingarnas gång lagt in reservationer om just obligatoriet att ta fram OSP och inrättandet av SLO. Även Sverige har i förhandlingarna verkat för att SLO inte ska vara obligatoriska för en ägare/förvaltare av en ECI men har under förhandlingarnas gång kunnat acceptera detta då det mer och mer lämnats upp till varje land att bestämma hur man ska organisera dessa.
[191] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

om kriterierna endast var riktgivande skulle förfaringssättet i de olika medlemsländerna sannolikt variera.[192]

Vad gäller eventuella nationella konsekvenser till följd av direktivet har samtliga länder som ingick i undersökningen gjort bedömningen att ett direktiv inte kommer att påverka det nationella arbetet på området nämnvärt. Som en direkt följd av detta har man heller inte vidtagit några särskilda åtgärder för att förbereda för en eventuell implementering av ett direktiv. Från många håll framgick att den dominerande uppfattningen var att liknande nationella system redan verkar finnas i många länder och att åtagandena som ett direktiv kan medföra därmed inte heller kommer att leda till några dramatiska förändringar och följaktligen inte heller bli så extremt dyra att genomföra. Intressant att notera i sammanhanget är att en granskning av Slovenien, Tjeckien och Frankrikes syn på eventuella konsekvenser till följd av ett direktiv kom fram till samma resultat då inte heller dessa tre länder ansåg att direktivet skulle medföra några omvälvande förändringar sett till det redan befintliga nationella CIP-arbetet.[193] Huruvida dessa bedömningar i samtliga fall verkligen är en följd av ett långtgående nationellt arbete på området eller om det kan ses som ett resultat av en ovetskap av vad som komma skall kan inte med säkerhet fastställas utifrån någon av dessa studier då en sådan bedömning hade krävt en grundläggande jämförelse av det faktiska CIP-arbetet. Att det finns vissa skillnader i de nationella systemen för skydd av kritisk infrastruktur vad gäller arbetets utformning, omfattning samt hur etablerade dessa är kan dock kasta viss tveksamhet över resultaten. Givet att det ännu inte har gått att komma överens om en definition av vad som är att betrakta som ECI framhålls också, med all rätta, att det är svårt för de nationella representanterna att bedöma vilket merarbete en implementering de facto kommer att kräva.

Av de granskade länderna har endast Nederländerna och Storbritannien studerat vilka konsekvenser ett direktiv kan komma att få nationellt men ingen av dessa analyser är offentliga. Inom ramen för den brittiska konsekvensanalysen har man bl.a. tittat på vad som görs nationellt, hur man skulle kunna genomföra direktivet och vilka konsekvenser det eventuellt skulle kunna få. Utöver det har man också haft workshops och möten med departementen som kommer att beröras av direktivet samt gjort en preliminär uppskattning av vad som eventuellt skulle kunna utpekas som europeisk kritisk infrastruktur i landet. I Nederländerna har man gjort bedömningen att en implementering av direktivet främst kommer att handla om en legislativ börda snarare än en budgetär sådan och har därför tillsatt en juridisk arbetsgrupp för att undersöka framförallt de legala konsekvenserna av ett direktiv. I Finland har man ännu inte gjort något motsvarande de brittiska eller holländska konsekvensanalyserna men man uppger sig ändå ha en generell idé kring vad ett direktiv kommer att innebära och hur man ska gå tillväga för att genomföra det.

---

[192] Intervju, tjänsteman vid det finska Inrikesdepartementet [14 december 2007] samt Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur) Helsingfors den 7 juni 2001.
[193] Åhman, (2008)

I den brittiska konsekvensbedömningen gjordes även en uppskattning av potentiella ECI inom landet. I runda slängar förväntar man sig att det kan komma att handla om drygt 10 stycken utpekade ECI men man betonar att detta endast är en preliminär bedömning och att det i slutändan beror på hur bred ECI-definitionen blir. Exempel på vad som bedömdes kunna bli utpekat som ECI på brittiskt territorium var exempelvis London som finansiellt centrum, energitillförsel/förråd med Irland samt energilänkar ner till kontinenten. När väl den slutliga ECI-definitionen är fastställd hoppas man från brittiskt håll att man inom hela EU totalt inte ska identifiera mer än drygt 100 ECI.[194] Då det råder osäkerheter kring hur europeisk kritisk infrastruktur ska definieras samt vilka kriterier som ska gälla för identifiering av europeisk kritisk infrastruktur uppgav såväl Finland som Nederländerna att det också är svårt att i dagsläget göra någon bedömning av hur många ECI man kommer att ha nationellt samt hur ett direktiv kommer att påverka det nationella arbetet kring skydd av kritisk infrastruktur. Generellt framhåller man dock från finsk sida att situationen i Norden skiljer sig från den i exempelvis Centraleuropa där länder av geografiska orsaker är mer sammankopplade till varandra.

Utifrån den brittiska uppskattningen av potentiella ECI i landet gjordes även en mer detaljerad granskning av dessa. En övergripande slutsats av detta arbete var att allt som man förväntade sig kunna bli utpekat som europeisk kritisk infrastruktur redan hade en säkerhetsplan samt en sambandsansvarig i säkerhetsfrågor motsvarande det som direktivets artikel fem och sex föreskriver och att implementeringskostnaderna därmed inte skulle bli särskilt höga.[195] Också Nederländerna och Finland drar liknande slutsatser gällande förekomsten av OSP och SLO. Från finskt håll framhåller man ändå att det är viktigt att de skyldigheter som åläggs verksamhetsutövarna genom direktivet inte innebär skyldigheter som är betydligt tyngre för de finländska verksamhetsutövarna än för närvarande till exempel i fråga om säkerhetsplanerna.[196]

Även om man i Finland inte har gjort någon utvärdering av de totala ekonomiska konsekvenserna av ett direktiv på området är den preliminära finska bedömningen att en implementering av direktivet inte kommer att bli särskilt kostsamt för staten. Detta trots att en princip i landet är att ägarna och operatörerna av vital infrastruktur bara behöver säkerställa sin verksamhet till en nivå som är affärsmässigt nödvändig och att den finska regeringen därutöver indirekt täcker eventuella merkostnader till följd av åtgärder för att höja skyddet för den vitala infrastrukturen.

---

[194] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]. Intressant att notera är att även slovenska företrädare har gett uttryck för att det kommer att finnas få ECI. Åhman (2008) s.54

[195] Dock noterade man att direktivet i sig också kan innebära en kostnad för ägarna/operatörerna att säkerställa att de följer lagen men det gjordes ingen uppskattning av hur mycket pengar det kan röra sig om i detta fall. Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

[196] Intervju, tjänsteman vid det finska Inrikesdepartementet [2007-12-12] samt Intervju, tjänsteman vid Försörjningsberedskapscentralen (FBC) [16 januari 2008]. Kommunikationsutskottets utlåtande över statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur) Dokumentreferens: 8/2007 rd.

Samtliga länder gör bedömningen att införandet av lagstiftning kommer att vara den största konsekvensen för deras befintliga nationella system för skydd av kritisk infrastruktur. I Finland har man gjort bedömningen att ett direktiv kommer att förutsätta ändringar i den sektorsvisa lagstiftningen, närmast i fråga om den planeringsskyldighet som åläggs företagen. Eventuellt kommer också den finska beredskapslagen och relaterad lagstiftning behöva justeras för att inkludera reglerna som direktivet för med sig men inga förberedelser har vidtagits härför.[197] Den danska bedömningen är att kravet om lagstiftning kan uppfyllas antingen genom att relevanta bestämmelser införs i redan existerande sektorslagstiftning eller genom att det införs en särskild lagstiftning om europeisk kritisk infrastruktur.[198] En brittisk högst preliminär uppskattning är att det kommer att kosta uppemot 10 miljoner euro att implementera lagstiftningskravet.[199]

Även om läsaren bör erinra sig om att endast ett begränsat antal personer har intervjuats inom ramen för denna studie och att urvalet av intervjuobjekt på just ministerienivå kan ha påverkat resultaten som framkommit, tyder de resonemang som förts av de nationella företrädarna på att man i samtliga medlemsstater tycks ta de faktiska implementeringskonsekvenserna med ro. En analys av studiens resultat ger vid handen att de granskade medlemsstaterna i sina argument emot direktivet tycks ha byggt upp sina ställningstaganden på principiella argument om vad som ska hanteras på nationell nivå och vad som ska skötas på EU-nivå snarare än någon bedömning av att direktivet kommer att medföra omvälvande förändringar som kommer att bli svåra att genomföra i förhållande till det redan befintliga nationella arbetet.

[197] Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur), Helsingfors den 7 juni 2007.
[198] Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007].
[199] Intervju, tjänsteman vid det brittiska Inrikesdepartementet [9 januari 2008]

9 VÄGEN FRAMÅT

EU:s samarbete på krisberedskapsområdet har intensifierats de senaste åren och trenden tycks peka mot allt fler sektorsövergripande strukturer och program vilka kan resultera i bindande lagstiftning och andra nationella åtaganden. Samtidigt som EU-samarbeten som dessa tillför mycket till det gemensamma säkerhetsarbetet innebär de samtidigt åtaganden som får konsekvenser på den nationella arenan.

I sin rapport ”Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys” belyser forskarna Pär Eriksson och Svante Barck-Holst hur det svenska arbetet med skydd av kritisk infrastruktur kan komma att påverkas av en gemensam EU-politik på området. Författarna sammanfattar att betydande utmaningar kan uppstå när man ska jämka samman det svenska decentraliserade systemet med det slags system som nu diskuteras på EU-nivå. Bland de viktigaste utmaningarna att uppmärksamma är enligt författarna den svenska myndighetsstrukturen som bygger på myndigheter med ett betydande sektorsansvar och KBM med en övergripande samordningsroll. Författarna påpekar vidare att ett sektorsövergripande system bl.a. skulle väcka frågor om vilken myndighet som ska representera Sverige i utvecklingen, vilka myndigheter som ska delta i implementeringen av ett sektorsövergripande system och slutligen hur sektorsövergripande analyser och direktiv ska föras in i det svenska systemet utan att sektorsmyndigheterna blir marginaliserade. En annan utmaning som författarna uppmärksammat är eventuella svenska kontra europeiska prioriteringarna av vad som ska skyddas. Författarna argumenterar här för att en gemensam europeisk hotbild samtidigt som det kan öka den gemensamma förståelsen och kunskapen också kan bidra till att likrikta åtgärder över hela EU som inte är relevant pga. skilda geografiska eller klimatologiska förhållanden. Slutligen lyfter författarna fram potentiella förändringar i relationen till ägare och operatörer som en tänkbar utmaning då dialogen på nationell nivå idag sker genom sakansvariga myndigheter men som i framtiden kan komma att bli mer centraliserade.[200]

Då ett direktiv om skydd av europeisk kritisk infrastruktur kan få såväl administrativa som finansiella och juridiska implikationer för Sverige måste en bred diskussion föras på hemmaplan med berörda myndigheter, mellan olika sektorer, i samverkansområdena samt med experter och den privata sektorn. I ljuset av rapportens resultat torde det bland annat vara önskvärt att även Sverige gör en grundlig nationell konsekvensanalys samt för en diskussion kring potentiella ECI inom landet. För det senare skulle exempelvis de av kommissionen tre prioriterade sektorerna transporter, telekommunikationer och energi med fördel först kunna studeras.[201] Ett ingångsvärde här skulle kunna vara att först identifiera nyckelmyndigheter inom dessa tre sektorer för att sedan genomföra intervjuer med dessa kring

[200] Eriksson, Barck-Holst (2005), s.11f.

[201] Dessa tre sektorer hade vidare kunnat brytas ner i ett antal underkategorier där exempelvis kommunikationer skulle kunna brytas ner i datakommunikationer, fast kommunikation, e-post, offentlig information och trådlös kommunikation medan transporter på ett liknande sätt skulle kunna delas in i flyg, marin, järnvägar och vägar. Energisektorn skulle slutligen kunna delas upp i elektricitet, naturgas och råolja.

vad som eventuellt skulle kunna tänkas bli utpekat som ECI inom deras respektive sektorer. Givet att definitionerna för vad som är att betrakta som ECI fortfarande saknas är en möjlighet att analysera konsekvenserna utifrån en omfattande såväl som en mindre omfattande definition av europeisk kritisk infrastruktur. En identifiering och inventering av potentiella ECI skulle förhoppningsvis bidra till att synliggöra vad vi har för luckor i det nationella arbetet med skydd av kritisk infrastruktur. Man kan exempelvis tänka sig att undersöka huruvida ägare och operatörer av potentiella ECI i landet redan har något liknande de säkerhetsplaner och sambandsansvariga i säkerhetsfrågor som direktivet stipulerar. Man kan därigenom få en indikation på vilka områden förändringar är att vänta samt hur omfattande dessa förändringar kommer att bli. I samband med detta är ett naturligt fortsättningssteg att titta närmare på vilka organisatoriska effekter ett direktiv kan få på det befintliga nationella arbetet i mer generella termer. Det kan exempelvis handla om att genomföra en konsekvensanalys där man tittar på hur sakområdena och de befintliga arbetsprocesserna kommer att påverkas, dvs. ansvarsfördelningen mellan ägare och operatörer av ECI och sektorsmyndigheterna, relationen mellan Regeringskansliet och den nya myndigheten för samhällets skydd och beredskap samt EPCIP:s inverkan på befintlig lagstiftning, finansiering och varningssystem. Detta arbete kan i sin tur fungera som en grund i framtagandet av en nationell CIP-strategi där man kan tänka sig att implementeringen av EPCIP endast utgör en del i en bredare nationell strategi. En viktig del i den fortsatta processen är att löpande hålla berörda aktörer informerade och delaktiga i arbetet genom exempelvis workshops och kontinuerliga möten med sektorsmyndigheterna, Regeringskansliet och ägarna/operatörerna av ECI.

Källförteckning

Litteratur

Brömmelhörster, J; Fabry, S; Wirtz, N; (2003) "Critical Infrastructure Protection: Survey of World-Wide Activities". Das Bundesamt für Sicherheit in der Informationstechnik (BSI). Tillgänglig online: http://www.bsi.de/

Fritzon, Ljungkvist, Boin, Rhinard (2007), "Protecting Europe's Critical Infastrucure: Problems and Prospects". Journal of Contingencies and Crisis Management, Volym 15, Nummer 1, Mars 2007.

Stein, W; Hämmerli, B; Pohl, H; och Posch, R; "Critical Infrastructure Protection (CIP) – status and perspectives". Preprints of the First GI Workshop on CIP, Frankfurt a.M. (2003) Tillgänglig online: http://www.gi-ev.de/fachbereiche/sicherheit/fg/kritis/CIP-Workshop-GI-03.pdf [2008-01-03]

Wenger, A; Metzger, J (ed.) (2004), "International CIIP Handbook 2004. An Inventory and Analysis of Protections Policies in Fourteen Countries". Swiss Federal Institute of Technology Zürich 2004.

Wenger, A. Mauer, V. (2006) "International CIIP Handbook 2006. An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies". Vol I och Vol II. Center for Security Studies. ETH Zürich

Offentligt tryck

Regeringskansliets faktapromemoria 2005/06:FPM43

Förordningen (2006:942) om krisberedskap och höjd beredskap

Sjöstrand, M; "Alltid redo! En ny myndighet mot olyckor och kriser" SOU 2007:31.

EU

Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism. Brussels 2004-10-20. COM (2004) 702 Final.

Commission Report "Results of the EPCIP Green Paper consultation Responses of the Member States". JLS/D1/PR/vdb D(2006) 4675, Brussels, 03/14/2006
Council conclusions on Principles for the European Programme for Critical Infrastructure Protection, 14766/05.

Förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna, Bryssel den 12.12.2006 KOM (2006) 787, slutlig. 2006/0276 (CNS). (Den senaste versionen från kommissionen är daterad 19 februari 2008. 5051/2/08 REV 2.)

Green paper on a European program for critical infrastructure protection, COM(2005) 576 final.

KOM/2005/576 av den 17 november 2005, grönbok om ett europeiskt program för skydd av kritisk infrastruktur.

Meddelande från kommissionen om ett europeiskt program för kritisk infrastruktur, Bryssel den 12.12.2006 KOM (2006) 786 slutlig.

Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, October 19 2007 (14083/07).

Krisberedskapsmyndigheten (KBM)

Enberg, J; Lundström, M; Kasström, H; ”Ett svenskt CIP-koncept” Promemoria, KBM [2007-07-07] (ej publicerad)

”Samhällsviktigt! – Ett första förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv” från den 31 januari 2006. KBM:s Dnr 0253/2005. Skriften kan laddas ner från Krisberedskapsmyndighetens webbplats www.krisberedskapsmyndigheten.se

“International CEP Handbook 2006. Civil Emergency Planning in the NATO/EAPC Countries”. KBM:s temaserie 2006:1. Krisberedskapsmyndigheten 2006.

”Krisberedskap i omvärlden. Samordningsstrukturer i fem länder”. KBM:s temaserie 2003:3. Krisberedskapsmyndigheten 2003.

Totalförsvarets forskningsinstitut (FOI)

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

Jarlsvik, H; Jönsson, T. (2005) ”Krisberedskapsmyndigheten och Europeiska unionen”. Totalförsvarets forskningsinstitut (FOI) [FOI-R—1654—SE].

Jarlsvik, H. Jönsson, T. (2005) ”Krisberedskapsmyndigheten och Europeiska unionen – en analys av hur KBM skulle kunna delta i EU-arbetet”. Totalförsvarets forskningsinstitut (FOI) Försvarsanalys [FOI-R--1654-SE].

Kjellén, S. (2007) ”Redovisning av EU:s varningssystem”. Krisberedskapsmyndigheten dnr 1067/2007

Åhman, T. (2008) ”Frankrike, Tjeckien och Slovenien – Tre perspektiv på EU:s krisberedskap”. Krisberedskapsmyndigheten dnr 1281/2007

Övrigt

Mötesanteckningar från PROCIV den 19 mars 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 23-24 maj 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 24-25 juli 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 13-14 september 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 8-9 oktober 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 19 oktober 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 19-20 november 2007 samt CIP contact group meeting 21 november 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 10 december 2007 (ej publicerade)

Mötesanteckningar från PROCIV den 18 januari 2008 (ej publicerade)

Mötesanteckningar från PROCIV den 12 februari 2008 (ej publicerade)

EU-upplysningen. Tillgänglig online: www.eu-upplysningen.se

DANMARK

Beredskabsstyrelsen, (BRS) hemsida Tillgänglig online: http://www.brs.dk/

Beredskabsstyrelsen, (BRS) ”Helhedsorienteret beredskabsplanlaegning, information, inspiration og praktik” [oktober 2005]

Danish comments on green paper on a European Programme for Critical Infrastructure Protection (presented by the commission).

Danish comments on green paper on a European Programme for Critical Infrastructure Protection (EPCIP). Beredskabsstyrelsen [1 juli 2005]

Denmark’s response to the Green Paper on a European Programme for Critical Infrastructure Protection. Beredskabsstyrelsen [30 januari 2006] Tillgänglig online: http://www.folketinget.dk/samling/20051/almdel/REU/spm/193/svar/endeligt/20060224/250943.PDF

DK non-paper EPCIP (ej publicerat)

”Et robust og sikkert samfund – Regeringens politik for beredskabet i Danmark”, juni 2005. Tillgänglig online: http://forsvaret.dk/NR/rdonlyres/F43B7906-C47C-4198-8358-5017A107000F/0/regeringenBeredskab5.pdf

Fakta blad, “Den civile sectors beredskab”, Beredskabsstyrelsen [2007-11-15] Tillgänglig online: http://www.brs.de

International CEP Handbook 2006. Civil Emergency Planning in the NATO/EAPC Countries. SEMA´s Educational Series 2006:1 Denmark p. 57-60

KBM:s landunderlag: Bilaga A, Danmarks krishanteringssystem [2006-02-06] samt [2007-08-15] Krisberedskapsmyndigheten (ej publicerade)

Regeringens redegorelse om beredskabet, maj 2007. [2007-11-15] Tillgänglig online: http://forsvaret.dk/NR/rdonlyres/554736F8-FC0B-44F9-AAD9-0FA3022F7187/46906/150507redegorelseomberedskabet.pdf

Udenrigsministeriets information om EPCIP till Folketingets försvars- och rättsutskott [11 januari 2007]. Tillgänglig online: http://www.eu-oplysningen.dk/upload/application/pdf/adad5c0b/787.pdf

Udenrigsministeriets information om EPCIP till Folketingets försvars-, europa- och rättsutskott [6 mars 2007]. Tillgänglig online: http://www.eu-oplysningen.dk/upload/application/pdf/adad5c0b/20060787.pdf

FINLAND

Intervjuer

Intervju, tjänsteman vid finska Inrikesdepartementet [2007-12-14]

Intervju, tjänsteman vid Försörjningsberedskapscentralen (FBC) [2008-01-16]

Övrigt material

”CIP – Kriittisen infrastruktuurin turvaaminen”, Huoltovarmuuskeskus Julkaisuja 1/2005, Axel Hagelstam. Tillgänglig online: http://www.huoltovarmuus.fi/documents/3/CIP-raportti_final.pdf [2007-10-24] (Rapporten finns inte tillgänglig på svenska men har en kort sammanfattning på engelska resp. svenska)

Finlands säkerhets- och försvarspolitik 2004. Statsrådets redogörelse SRR 6/2004. Tillgänglig online: http://www.defmin.fi/files/178/2552_2162_Den_fOrsvarspolitiska_redogOrelsen_2004_1_.pdf

Hallintovaliokunnan lausunto 19/2007 vp. (Förvaltningsutlåtande) Helsingfors 9 november 2007. Tillgänglig online: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/havl_19_2007_p.shtml (Dokumentet FvUU 19/2007 finns inte på svenska.)

Kommunikationsutskottets utlåtande 8/2007 rd om statsrådets skrivelse om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Helsingfors den 28 september 2007 Tillgänglig online: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/kouu_8_2007_p.shtml

Programmet för den inre säkerheten. Tillgänglig online: http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/pages/indexsve

Promemoria, ”Förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna”. Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur). Konsultativ tjänsteman Jukka Metso. Helsingfors den 7 juni 2007 Tillgänglig online: http://217.71.145.20/TRIPviewer/temp/TUNNISTE_U_12_2007_ru.html [2008-01-08]

Statsrådets principbeslut om målen för den nationella informationssamhällspolitiken 2007–2011. Tillgänglig online: http://www.mintc.fi/oliver/upl799-Principbeslut.pdf

Statsrådets skrivelse till riksdagen om ett förslag till rådets direktiv (europeisk kritisk infrastruktur) Helsingfors den 7 juni 2007 [07.06.2007] Tillgänglig online: http://217.71.145.20/TRIPviewer/show.asp?tunniste=U+12/2007&base=erur&palvelin=www.eduskunta.fi&f=WORD&kieli=ru

Statsrådets utredning med anledning av ett förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna [07.02.2007]

Statsrådets principbeslut om tryggande av samhällets livsviktiga funktioner (2003). Tillgänglig online: http://www.defmin.fi/files/182/2566_1688_Principbeslut_1_.pdf

Strategi för tryggande av samhällets livsviktiga funktioner (2003) Helsingfors 21 november 2003. Tillgänglig online: http://www.defmin.fi/files/126/2566_1688_Strategi_fOr_tryggande_av_samhAllets_livsviktiga_funktioner_1_.pdf

Strategi för tryggande av samhällets livsviktiga funktioner (2006) Helsingfors 23 november 2006. Tillgänglig online:

http://www.defmin.fi/files/872/Strategi_for_tryggande_av_samhallets_vitala_funktioner_2006.pdf

Talousvaliokunnan lausunto 13/2007 vp. (Ekonomiutlåtande) Helsingfors 12 oktober 2007. Tillgänglig online:
http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/tavl_13_2007_p.shtml
(Dokumentet EkUU 13/2007 finns inte på svenska)

NEDERLÄNDERNA

Intervjuer

Intervju, tjänsteman vid nederländska Inrikesdepartementet [12 december 2007]

Intervju, forskare vid the Netherlands Organisation for Applied Scientific Research (TNO), Department for Defense, Security and Safety [21 januari 2008]

Övrigt material

Luiijf, E; Burger, H; Klaver, M; "Critical Infrastructure Protection in The Netherlands: A Quick-scan". TNO Physics and Electronics Laboratory (TNO-FEL), The Netherlands (2003) Tillgänglig online:
http://cipp.gmu.edu/archive/2_NetherlandsCIdefpaper_2003.pdf

Luiijf, E; "Critical Infrastructure Protection: R&D view". European Conference on Security Research SRC07, Berlin, 26/03/07 Tillgänglig online:
http://www.hcss.nl/en/publication/330/Critical-Infrastructure-Protection:-R&D-view.html

Nederländska Inrikesdepartementet Tillgänglig online: www.minbzk.nl/uk/ [2007-11-09]
samt www.minbzk.nl/veiligheid/nationaal/inspringthema_s/expertisecentrum [2007-11-09]

The Netherlands Organisation for Applied Scientific Research (TNO),
Tillgänglig online: www.tno.nl [2007-11-09]

"Report on Critical Infrastructure Protection - The Dutch approach on CIP". (2004)
Tillgänglig online: http://www.fbiic.gov/reports/neth_4.pdf

"Critical Infrastructure Protection: Issues for Resilient Design". KBM reserapport från konferens i Nederländerna – den 18-19 april 2007. (ej publicerad)

STORBRITANNIEN

Intervjuer

Intervju, tjänsteman vid brittiska Inrikesdepartementet [9 januari 2008]

Internetmaterial

Centre for the Protection of National Infrastructure, CPNI
http://www.cpni.gov.uk/

The Civil Contingencies Secretariat, CCS
http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx

The Central Sponsor for Information Assurance, CSIA

http://www.cabinetoffice.gov.uk/csia.aspx

The Defence Research Centre, DSTL
http://www.dstl.gov.uk/index.php

The Information Assurance Advisory Council, IAAC
http://www.iaac.org.uk/

BILAGA I

Tabell: Sammanställning av olika länders/organisationers definition av kritisk infrastruktur

Organisationer	Definition på kritisk infrastruktur
Europeiska unionen (EU)	"Critical Infrastructure" means 1. those assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; or 2. those hazardous assets, systems or parts thereof located in the EU Member States the disruption or destruction of which would, as a direct consequence, have a significant impact in a Member State regardless of any impact due to the loss of service from that infrastructure. "European Critical Infrastructure" means critical infrastructure located in the EU Member States the disruption or destruction of which would have a significant impact on two or more Member States, or a single Member State if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure; The list of critical infrastructure sectors includes; (1) energy, (2), nuclear fuel-cycle industry (for radiological hazard) (3) information and communication technologies, (4) water, (5) food, (6) health, (7) financial, (8) transport, (9) chemical industry, (10) space and (11) research facilities. (Källa: Förslag till rådets direktiv om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna. Den senaste versionen från kommissionen är daterad 19 februari 2008. 5051/2/08 REV 2.)
North Atlantic Treaty Organisation (NATO)	"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." (Källa: Working definition for critical infrastructure which was developed by the CPC and endorsed By the SCEPC on 4 November 2003)
Länder	**Definition på kritisk infrastruktur**
Danmark	"[Kritisk infrastruktur] kan forstås som de elementer i et overordnet system (samfund), der er så vitale, at forstyrrelse og nedbrud af bare en enkelt af dem ville kunne true selve systemets funktionsduelighed". (Källa: Beredskabsstyrelsen)
Finland	I den finländska strategin för tryggande av samhällets livsviktiga funktioner identifieras sju samhällsviktiga funktioner: (1) Ledning av staten, (2) internationell verksamhet, (3) det militära försvaret av riket, (4) upprätthållande av den inre säkerheten, (5) ekonomins och infrastrukturens funktionsförmåga, (6) befolkningens försörjning och handlingsförmåga samt (7) mental kristålighet. Inom dessa sju kritiska sektorer identifieras i sin tur kritiska tjänster/produkter. (Källa: Försörjningsberedskapscentralen, FBC)
	"A product or service is vital when it either: provides an essential contribution to society in

Nederländerna	maintaining a defined minimum quality level of (1) national and international law & order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or when loss or disruption impacts citizens or government administration at a national scale or endangers the minimum quality level". I Nederländerna startade quick scan arbetet 2002 och då identifierades 11 kritiska sektorer och 31 kritiska produkter och tjänster. Efter april 2004 har man identifierat 12 vitala sektorer med sammanlagt 33 kritiska tjänster och produkter; (1) energi, (2) telekommunikationer, (3) dricksvatten, (4) livsmedel, (5) hälsa/hälsovård, (6) finansväsendet, (7) kontroll av ytvattnets kvalitet och kvantitet, (8) allmän ordning och säkerhet, (9) rättsordning, (10) offentlig administration, (11) transport och (12) kemisk och nukleär industri. (Källa: Nederländska Inrikesministeriet, "Quick Sacan on Critical Products and Services" samt CIIP handbook 2006)
Storbritannien	I Storbritannien talar man om "Critical National Infrastructure". "The [Critical National Infrastructure (CNI)] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: cause large-scale loss of life, have a serious impact on the national economy, have other grave social consequences for the community or be of immediate concern to the national government." There are nine sectors which deliver essential services: (1) energy, (2) food, (3) water, (4) transport, (5) telecommunications, (6) government & public services, (7) emergency services, (8) health and (9) finance. Within these sectors there are key elements that comprise the critical national infrastructure. These are the components or assets without which the essential services cannot be delivered. These components may be physical or electronic. CPNI works with the operators of essential services and with lead government departments to identify critical national infrastructure within the nine sectors, and to help protect it against national security threats. Enligt det nuvarande sättet att beteckna nationell kritisk infrastruktur har man identifierat 9 sektorer som är kritiska för landet; (1) energi, (2) livsmedel, (3) vatten, (4) transport, (5) telekommunikationer, (6) offentlig förvaltning och service, (7) räddningstjänst, (8) hälsa och (9) finans. (Källa: Centre for the Protection of National Infrastructure, CPNI)
Sverige	I Sverige använder Krisberedskapsmyndigheten (KBM) begreppet "samhällsviktig verksamhet" som bör avse en verksamhet som uppfyller båda eller det ena av följande villkor: 1.) Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. 2.) Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället skall kunna hanteras så att skadeverkningarna blir så små som möjligt. Som exempel på sektorer där det finns verksamheter som alltid måste fungera nämns: (1) energiförsörjning, (2) vattenförsörjning, (3) information och kommunikation, (4) finansiella tjänster, (5) socialförsäkringar, (6) hälso- och sjukvård, (7) social omsorg, (8) skydd och säkerhet, (9) transporter, (10) kommunalteknisk försörjning, (11) livsmedel, (12) handel och industri samt (13) offentlig förvaltning. Man betonar att det är viktigt att regelbundet analysera vad som är samhällsviktiga verksamheter i olika situationer eftersom vad som är samhällsviktigt kan variera dels över tid, dels beroende på vilken krissituation det handlar om.

	(Källa: KBM ”Samhällsviktigt!”)
USA	I USA använder man termen “critical infrastructure and key resources” (CI/KR). Critical infrastructure are “[a]ssets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.” CIKR is organized into 17 sectors that together provide essential functions and services supporting various aspects of the U.S. Government, economy, and society: (1) agriculture and food, (2) defense industrial base, (3) energy, (4) public health and healthcare, (5) national monuments and icons, (6) banking and finance, (7) drinking water and water treatment systems, (8) chemical, (9) commercial facilities, (10) dams, (11) emergency services, (12) nuclear reactors, materials and waste, (13) information technology, (14) communications, (15) postal and shipping, (16) transportation systems and (17) government facilities. Policies for CIKR protection and preparedness are established through the following authorities: Homeland Security Act of 2002; Homeland Security Presidential Directive (HSPD), ‘Critical Infrastructure Identification, Prioritization, and Protection’; the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets; the National Strategy for Securing Cyberspace; and other relevant statutes, Executive orders, and Presidential directives. (Källa: the Federal Emergency Management Agency (FEMA)

Kommentar: Definitionerna för de olika länderna är hämtade från Försörjningsberedskapscentralen (Finland), Inrikesdepartementet (Nederländerna), Centre for the Protection of National Infrastructure, CPNI (Storbritannien), Krisberedskapsmyndigheten (Sverige), Beredskabsstyrelsen (Danmark) samt the Federal Emergency Management Agency (FEMA) (USA).