

# EUROPAPARLAMENTET

2004



2009

---

*Utskottet för ekonomi och valutafrågor*

PRELIMINÄR VERSION  
**2006/0276(CNS)**

21.3.2007

## FÖRSLAG TILL YTTRANDE

från utskottet för ekonomi och valutafrågor

till utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes  
frågor

över förslaget till rådets direktiv om kartläggning och klassificering av  
europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av  
denna  
(KOM(2006)0787 – C6-0053/2007 – 2006/0276(CNS))

Föredragande: Harald Ettl

PA\_Legam

## KORTFATTAD MOTIVERING

Kommissionen har med beaktande av Haagprogrammet av den 5 november 2005, vilket omfattar både en effektiv hantering av gränsöverskridande kriser och ett förbättrat katastrofskydd och skydd av kritisk infrastruktur för unionen i kampen mot terrorismen, och med beaktande av kommissionens förberedande arbete inom ramen för grönboken av den 17 november 2005, lagt fram ett förslag om planerade förbättringsåtgärder av den europeiska krishanteringen.

Kritisk infrastruktur är fysiska resurser och IT-kapacitet, nät, tjänster och anläggningstillgångar, som om de störs eller förstörs kan få allvarliga konsekvenser för hälsan, säkerheten eller medborgarnas ekonomiska välbefinnande samt för effektivt fungerande regeringar i medlemsstaterna. Kritisk infrastruktur finns i flera näringslivssektorer, bland annat i bank- och finanssektorn, i transport- och distributionssektorn, på områdena energi, försörjningsföretag, hälsa, livsmedelsförsörjning och kommunikation och de viktiga offentliga tjänsterna.

Skyddet av kritisk infrastruktur i EU är tillsammans med den inre säkerheten en central fråga för det europeiska samhällssystemet. Förstörelse av kritisk infrastruktur kan ur psykologisk synvinkel leda till en fullkomlig förlust av allmänhetens förtroende för EU. De enskilda medlemsstaternas krishantering befinner sig för närvarande på ytterst olika nivåer. Avsikten med det aktuella förslaget från kommissionen är att särskilt av detta skäl kartlägga europeisk kritisk infrastruktur och klassificera den genom ett gemensamt förfarande.

En förutsättning för en aktiv krishantering är att alla nödvändiga kommunikationssystem på IT- och telekommunikationsområdet upprätthålls. Dessa sektorer kännetecknas av en tvärsnittsmässig infrastruktur och utgör samtidigt en kritisk infrastruktur för andra kritiska infrastrukturer, såsom för penning-, finans- och försäkringsväsendena. Ett riktat angrepp mot datanätet hos ECB, en storbank eller Frankfurtsbörsen måste kunna motverkas snabbt i tekniskt och institutionellt avseende.

För stora koncerner är gränsöverskridande arbete oundvikligt. En europeisk undersökning från 2000 visade att mer än hälften av de berörda företagen inte genomför några säkerhetsanalyser. Det eventuella missbruket av webbservrar underlättar också radikal aktionism och är en viktig beståndsdel i terroristisk informationsteknik.

Infrastrukturer med en internationell dimension och dåliga tillgängliga alternativ är särskilt sårbara vid alla typer av katastrofer. Denna sårbarhet märktes särskilt tydligt vid strömavbrottet i det europeiska överföringsnätet den 4 november 2006. Vattenförsörjningen med grund-, käll- och rinnande vatten som också är gränsöverskridande och mellanstatlig kan trots nationella nät utvecklas till ett försörjningsproblem.

Även järnvägstrafik med gränsöverskridande förbindelser och flygplatser med flygsäkerhetsanläggningar måste i krissituationer kunna förlita sig på europeisk logistik för motåtgärder.

Försäkrings- och återförsäkringsföretag har till följd av sin bransch sedan många år ägnat sig åt riskhanteringsfrågor. I direktiv, såsom inom ramen för riktlinjerna i åtgärds paketet

”solvens I”, har hänsyn redan tagits till riskhanteringsfrågor för försäkringar både när det gäller datafrågan och den materiella täckningsgraden, och måste anpassas till den faktiska situationen när det gäller de ökade riskerna i solvens II-projektet. För försäkringar måste trots den nödvändiga proportionaliteten en ytterligare – eventuellt också en statlig – risk för skadeståndsanspråk tas med i diskussionerna.

Föredraganden välkomnar och ger sitt stöd till kommissionens avsikt att samordna åtgärderna för skyddet av kritisk infrastruktur på europeisk nivå. Det måste emellertid påpekas att en dubbling av befintliga sektorsåtgärder måste förhindras, t.ex. de bestämmelser som finns i rekommendationerna för värdepappersavvecklingssystem, för standarder för clearing och avveckling av värdepapper i EU och standarderna för användning av värdepappersavvecklingssystem i EU vid transaktioner inom ramen för ECBS.

Ur kombinationen av bindande och icke-bindande åtgärder måste det utarbetas en realistisk kostnadseffektivitet för ett europeiskt mervärde.

## ÄNDRINGSFÖRSLAG

Utskottet för ekonomi och valutafrågor uppmanar utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor att som ansvarigt utskott infoga följande ändringsförslag i sitt betänkande:

Kommissionens förslag

Parlamentets ändringar

### Ändringsförslag 1 Skäl 5a (nytt)

***(5a) I vissa sektorer finns det redan en rad åtgärder som reglerar kartläggningen, klassificeringen och skyddet av kritisk infrastruktur. En framtida lagstiftning på EU-nivå får inte leda till en parallell ordning – om inte en sådan medför att extra säkerhet uppnås.***

### Ändringsförslag 2 Artikel 1

Genom detta direktiv fastställs ett förfarandet för kartläggning och klassificering av europeisk kritisk infrastruktur och en gemensam metod för bedömning av behovet av ett stärkt skydd

Genom detta direktiv fastställs ett förfarandet för kartläggning och klassificering av europeisk kritisk infrastruktur och en gemensam metod för bedömning av behovet av ett stärkt skydd

för sådan infrastruktur.

***mot alla typer av hot*** för sådan infrastruktur.

#### *Motivering*

*Strategin bör vara att ha ett skydd mot alla typer av hot, även hot som varken beror på terrorism eller naturkatastrofer, men som trots det varaktigt kan påverka infrastrukturens funktionsduglighet och integritet. Hit hör bland annat mänskliga fel, otillräckligt kvalificerad personal, utläggande på entreprenad av företagskritiska infrastrukturer, epidemier/sjukdomar, ökat IT-beroende, världsomfattande sammankopplingar av IT-system, politisk instabilitet och så vidare.*

#### Ändringsförslag 3

##### Artikel 5, punkt 2, stycke 1

Säkerhetsplan skall kartlägga anläggningarna inom den europeiska kritiska infrastrukturen och fastställa lämpliga säkerhetslösningar för att skydda dessa anläggningar enligt bilaga II. Sektorsspecifika krav gällande säkerhetsplanen som avser befintliga gemenskapsåtgärder kan ***antas*** i enlighet med det förfarande som avses i artikel 11.3.

Säkerhetsplan skall kartlägga anläggningarna inom den europeiska kritiska infrastrukturen och fastställa lämpliga säkerhetslösningar för att skydda dessa anläggningar enligt bilaga II. Sektorsspecifika krav gällande säkerhetsplanen som avser befintliga gemenskapsåtgärder kan ***beaktas till fullo*** i enlighet med det förfarande som avses i artikel 11.3.

#### *Motivering*

*Försäkringsföretag och banker tillhör de branscher som kontinuerligt investerar stora belopp i säkerhetsanordningar såsom tillgångskontroller eller säkring av informationssystem. De statliga åtgärderna får inte innebära en dubbling av redan befintliga sektorsåtgärder. Därför bör en framtida lagstiftning i full utsträckning ta med befintliga säkerhetsplaner.*

#### Ändringsförslag 4

##### Artikel 10, punkt 3

3. Medlemsstaterna skall säkerställa att information om skyddet av kritisk infrastruktur som lämnas till medlemsstaterna eller kommissionen inte används i något annat syfte än för att skydda kritisk infrastruktur.

3. Medlemsstaterna skall säkerställa att information om skyddet av kritisk infrastruktur som lämnas till medlemsstaterna eller kommissionen inte används i något annat syfte än för att skydda kritisk infrastruktur ***och att hänsyn o villkorligen även tas till proportionalitetsprincipen i ekonomiskt hänseende och grundläggande rättigheter och institutioner som bör skyddas.***

## *Motivering*

*Till andra grundläggande rättigheter och institutioner som bör skyddas hör till exempel uppgiftsskydd och telekommunikationshemligheter.*

### Ändringsförslag 5 Bilaga I, sektor VII ”Finans”, delsektor 19

19. Clearing- och avvecklingssystem för betalningar och värdepapper samt tillhörande system *(Berör inte den svenska versionen.)*

### Ändringsförslag 6 Bilaga I, sektor VII ”Finans”, delsektor 19a (ny)

#### ***19a. Betalningssystem***

### Ändringsförslag 7 Bilaga I, sektor VII ”Finans”, delsektor 19b (ny)

#### ***19b. Bank och försäkring***