EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 27.10.2008
SEK(2008) 2702

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

Följedokument till

förslag till

RÅDETS BESLUT

om inrättande av nätverket för varningar om hot mot kritisk infrastruktur (Ciwin)

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

{COM(2008) 676 final}
{SEC(2008) 2701}

Den 6 juni 2008 avgav kommissionens konsekvensbedömningsnämnd ett yttrande om en preliminär version av konsekvensbedömningsrapporten. Nämnden ansåg att rapporten var avfattad på ett klart och även för andra än fackmän begripligt språk och att den gav en ingående analys av den möjliga utformningen av nätverket. I huvudrekommendationerna i yttrandet angav nämnden att de befintliga systemen för snabb varning (*rapid alert systems*, RAS) i medlemsstaterna borde beskrivas bättre i rapporten och att fördelarna med Ciwin borde redovisas tydligare i denna.

Nämnden ansåg också

- att huvudscenariot borde utvecklas och Ciwininitiativets mervärde framhävas, och
- att medlemsstaternas upptagning av initiativet borde analyseras i rapporten.

1. CIWININITIATIVET

Ciwininitiativet utgör en del av det europeiska programmet för skydd av kritisk infrastruktur (Epcip) och rör mer specifikt processen för utbyte av information medlemsstaterna emellan och det it-system som ska backa upp denna process. Förslaget om att inrätta Ciwin lades fram i meddelandet om Epcip (KOM(2006) 786 slutlig). I meddelandet redovisas den övergripande ramen för skyddet av kritisk infrastruktur i EU samt hur Epcip och Ciwin kan genomföras.

Rådet har ställt sig bakom kommissionens planer på att inrätta Ciwin (se ”Rådets slutsatser om förebyggande, beredskap och insatser när det gäller terroristattacker” och ”EU:s solidaritetsprogram om följderna av terroristhot och terroristattacker”, som antogs av rådet i december 2004[1]).

De viktigaste problemen för närvarande är

- behovet av en mer ingående bedömning av hur den kritiska infrastrukturen i EU ska skyddas,
- behovet av ett bättre samarbete och informationsutbyte EU-medlemsstaterna emellan om kritisk infrastruktur,
- överlappningar av verksamhet, och
- att de berörda parterna inte har tillräckligt mycket förtoende för varandra för att vilja utbyta känslig information.

2. MÅL

Den konkreta fråga som kräver åtgärder på EU-nivå är att underlätta informationsutbyte mellan medlemsstaternas myndigheter (t.ex. om bästa praxis) och göra det möjligt för dem att använda systemet för snabb varning på området skydd av kritisk infrastruktur.

[1] Rådets dok. 14894/04.

Målet med Ciwin är att bidra till att förbättra skyddet av kritisk infrastruktur i EU och underlätta samordning och samarbete på EU-nivå i fråga om information om skydd av kritisk infrastruktur.

De operativa målen för Ciwin är

- att tillhandahålla ett it-verktyg som hjälper de medlemsstater som vill samarbeta att göra detta,

- att erbjuda ett effektivt och snabbt alternativ till tidskrävande metoder för att söka efter information (dvs. att skapa ett slags ”one-stop shop” för all relevant information om kritisk infrastruktur i EU),

- att se till att den information som utbyts inte hamnar i fel händer, och

- att ge medlemsstaterna möjlighet att kommunicera direkt och ladda upp all information som de anser vara relevant.

Eftersom vissa medlemsstater skulle föredra att använda endast en del av de funktioner som Ciwin erbjuder, är det nödvändigt att finna en lösning som medger detta.

3. POLICYALTERNATIV

I konsekvensbedömningen togs följande fem policyalternativ i beaktande:

Ingen specifik policy

Inga övergripande åtgärder på europeisk nivå. Medlemsstaterna får ta itu med frågan på egen hand.

Ciwin som en uppgradering av de befintliga systemen för snabb varning

Med detta alternativ skulle Ciwin integrera de befintliga systemen för snabb varning i ett sektorsövergripande system för snabb varning på området skydd av kritisk infrastruktur. Systemet skulle vara tillgängligt för ett bredare spektrum av berörda parter än sektorsmyndigheter eller beredskapsorgan (såsom civilskydd eller sjukvård). Detta alternativ skulle emellertid inte medge utbyte av allmän information och bästa praxis.

Ciwin som en öppen plattform för (osäkrat) utbyte av information om skydd av kritisk infrastruktur

Detta alternativ kräver ett it-verktyg som är tillgängligt för allmänheten och fungerar som en vanlig webbplats. Det skulle säkert bidra till att göra allmänheten mer medveten om frågan om skydd av kritisk infrastruktur i Europa och öka det direkta informationsutbytet mellan de berörda parterna.

Ciwin som ett säkert, icke-obligatoriskt kommunikations- och varningssystem med ett flertal nivåer och två distinkta funktioner, nämligen ett system för snabb varning och ett elektroniskt forum för utbyte av idéer och bästa praxis på området skydd av kritisk infrastruktur

Detta alternativ kräver ett it-verktyg som kan lagra och överföra känslig information som sekretessbelagts upp till nivån *Restreint UE*. Utöver utbytet av idéer och bästa praxis i det elektroniska forumet skulle tonvikten ligga på dialog och uppbyggnad av förtroende på EU-nivå. Det skulle stå medlemsstaterna fritt att använda hela nätverket eller bara en av de båda funktionerna. De skulle också kunna avstå helt från att använda nätverket.

Ciwin som ett säkert, obligatoriskt kommunikations- och varningssystem med ett flertal nivåer och två distinkta funktioner, nämligen ett system för snabb varning och ett elektroniskt forum för utbyte av idéer och bästa praxis på området skydd av kritisk infrastruktur

Varje medlemsstat skulle vara skyldig att ladda upp och regelbundet uppdatera relevant information.

4. FÖR- OCH NACKDELAR MED DE OLIKA ALTERNATIVEN

Policyalternativ	Fördelar	Nackdelar
Alternativ 1: ingen specifik policy	Inget nytt förslag till rättsakt. Medlemsstaterna helt fria att hantera frågan om skydd av kritisk infrastruktur så som de anser lämpligt.	Ingen förändring i dialogen och informationsutbytet mellan medlemsstaterna. Inget enhetligt, säkert och effektivt it-system i Europa för utbyte av information om skydd av kritisk infrastruktur. Ingen inverkan på säkerheten i EU. Ingen garanti att alla berörda parter i Europa har tillgång till relevant information om skydd av kritisk infrastruktur.
Alternativ 2: uppgradering av de befintliga systemen för snabb varning	Inrättande av ett sektorsövergripande system för snabb varning.	Höga kostnader för att säkerställa de befintliga systemens interoperabilitet. Alternativet medger inte utbyte av information och bästa praxis. En ny plattform för utbyte av information behöver inrättas i vilket fall som helst.
Alternativ 3: öppen plattform för (osäkrat) utbyte av information om skydd av kritisk infrastruktur	Vid tillgång till information om skydd av kritisk infrastruktur. Den privata sektorn kan ge direkta bidrag.	Informationen i nätverket kommer att utgöras enbart av icke sekretessbelagd information. Eftersom sådan information redan finns tillgänglig, tillför detta

	Informationen i nätverket kommer visserligen att utgöras av information som redan är tillgänglig för allmänheten, men Ciwin skulle genom ett effektivt, samordnat tillträde göra det enklare att få tag i den.	alternativ inte mer än ett begränsat mervärde. Inga möjligheter att utbyta varningsmeddelanden.
Alternativ 4: säkert, icke-obligatoriskt kommunikations- och varningssystem med ett flertal nivåer och två distinkta funktioner	Nätverket skulle erbjuda en säker miljö för utbyte av information och bidra väsentligt till uppbyggnad av förtroende mellan de berörda parterna. Informationen i nätverket skulle utgöras av mera än sådant som redan är tillgängligt för allmänheten. Nätverket skulle göra det möjligt att utbyta varningsmeddelanden. Ciwin skulle utgöra ett effektivt it-system som skulle vara enkelt att använda. Ciwin skulle bidra till att förbättra säkerheten i EU. Ciwin skulle genom bättre samordning och utökat samarbete bidra till att undanröja fragmenteringen i forskningsverksamheten på området skydd av kritisk infrastruktur.	Berörda parter i den privata sektorn skulle inte ha direkt tillträde till Ciwin. Ciwins framgång skulle vara avhängig av medlemsstaternas vilja att använda nätverket.
Alternativ 5: säkert, obligatoriskt kommunikations- och varningssystem med ett flertal nivåer och två distinkta funktioner	Samtliga medlemsstater skulle delta i nätverket. Informationen i nätverket skulle utgöras av mera än sådant som redan är tillgängligt för allmänheten. Nätverket skulle göra det möjligt att utbyta varningsmeddelanden. Ciwin skulle utgöra ett effektivt it-system som skulle vara enkelt att	Medlemsstaterna skulle inte understödja förslaget. Ett obligatoriskt system torde inte bidra till uppbyggnad av förtroende och skulle misslyckas. Det är möjligt att ett obligatoriskt system strider mot proportionalitets-principen.

	använda. Ciwin skulle bidra till att förbättra säkerheten i EU. Ciwin skulle genom bättre samordning och utökat samarbete bidra till att undanröja fragmenteringen i forskningsverksamheten på området skydd av kritisk infrastruktur.	

5. PREFERENSALTERNATIV

Vid analysen av de fem alternativen uppvisade alternativ 4 – Ciwin som ett säkert, icke-obligatoriskt kommunikations- och varningssystem med ett flertal nivåer och två distinkta funktioner, nämligen ett system för snabb varning och ett elektroniskt forum för utbyte av idéer och bästa praxis på området skydd av kritisk infrastruktur – det klart mest gynnsamma förhållandet mellan för- och nackdelar.

Det bör betonas att Ciwin inte kommer att innebära någon omvälvning för säkerheten i EU och att nätverket måste betraktas som endast ett av många steg i genomförandet av det europeiska programmet för skydd av kritisk infrastruktur. Ciwin är ett it-verktyg som är avsett att underlätta kommunikation om frågor som rör skyddet av kritisk infrastruktur och kommer att erbjuda sådana funktioner som nyhetsanslagstavlor, diskussionsgrupper, samarbetsmiljöer (*collaborative environments*) och dokument- och arbetsflödeshantering, dvs. komponenter som hör till det dagliga umgänget med Internet eller företagsintranät. I arbetet med Ciwin kommer ett stort antal olika komponenter att tas i övervägande. Det kommer därvid också att ses till att dessa ska kunna tas bort ifall de inte verkar tillföra något mervärde eller ifall de är oförenliga med etablerad praxis.