KOMISIA EURÓPSKYCH SPOLOČENSTIEV

Brusel, 12.12.2006
KOM(2006) 787 v konečnom znení

2006/0276 (CNS)

Návrh

SMERNICA RADY

o identifikácii a označení európskej kritickej infraštruktúry a zhodnotení potreby zlepšiť jej ochranu

(predložená Komisiou)

{SEK(2006) 1648}
{SEK(2006) 1654}

DÔVODOVÁ SPRÁVA

1) KONTEXT NÁVRHU

- **Dôvody a ciele návrhu**

Európska rada na svojom zasadnutí v júni 2004 požiadala Komisiu, aby vypracovala celkovú stratégiu ochrany kritickej infraštruktúry. Komisia 20. októbra 2004 prijala Oznámenie o ochrane najdôležitejšej infraštruktúry v boji proti terorizmu, v ktorom predložila návrhy možných opatrení na zvýšenie úrovne prevencie teroristických útokov proti kritickej infraštruktúre (CI), pripravenosti a reakcie na ne.

Závery Rady o „Prevencii, pripravenosti a reakcii na teroristické útoky“ a „Program solidarity EÚ o dôsledkoch teroristických hrozieb a útokov“ prijatý Radou v decembri 2004 podporili zámer Komisie navrhnúť Európsky program na ochranu kritickej infraštruktúry (EPCIP) a vyjadrili súhlas s vytvorením Varovnej informačnej siete kritickej infraštruktúry (CIWIN).

V novembri 2005 Komisia prijala Zelenú knihu o Európskom programe na ochranu najdôležitejšej infraštruktúry (EPCIP), v ktorej predstavila možné scenáre uskutočnenia EPCIP a CIWIN.

V decembri 2005 Rada pre spoluprácu v oblasti spravodlivosti a vnútorných záležitostí vyzvala Komisiu, aby do júna 2006 predložila návrh EPCIP.

Tento návrh smernice predstavuje opatrenia, ktoré Komisia navrhuje v súvislosti s identifikáciou a označením európskej kritickej infraštruktúry a zhodnotením potreby zlepšiť jej ochranu.

- **Všeobecný kontext**

V Európskej únii existuje rad kritických infraštruktúr, ktorých narušenie alebo zničenie by ovplyvnilo dva alebo viaceré členské štáty. Taktiež sa môže stať, že výpadok kritickej infraštruktúry v jednom členskom štáte bude mať účinky v inom členskom štáte. Takéto kritické infraštruktúry nadnárodnej povahy by sa mali identifikovať a označiť ako európske kritické infraštruktúry (ECI). Toto je možné urobiť len prostredníctvom spoločného postupu týkajúceho sa identifikácie ECI a zhodnotenia potreby zlepšiť ich ochranu.

Vzhľadom na tento nadnárodný charakter by integrovaný prístup na úrovni EÚ pri zisťovaní slabých a zraniteľných miest a identifikovaní nedostatkov v ochranných opatreniach predstavoval vhodné doplnenie a prínos vo vzťahu k národným programom pre ochranu kritickej infraštruktúry, ktoré už existujú v členských štátoch, a bol by významným prínosom aj v súvislosti s ďalším trvaním európskeho vnútorného trhu a jeho schopnosťou vytvárať bohatstvo.

Keďže existujú rôzne sektory s osobitnými skúsenosťami, odbornými znalosťami a požiadavkami v súvislosti s ochranou kritickej infraštruktúry (CIP), mal by sa vyvinúť a presadiť prístup k CIP na úrovni EÚ, ktorý by zohľadňoval špecifiká jednotlivých sektorov vo vzťahu ku kritickej infraštruktúre (CI) a ktorý by vychádzal z existujúcich sektorovo špecifických opatrení. Vypracovanie spoločného zoznamu sektorov kritickej infraštruktúry je

nevyhnutné na to, aby sa uľahčilo presadenie sektorovo špecifického prístupu k ochrane kritickej infraštruktúry.

- **Potreba spoločného rámca**

Len spoločný rámec môže poskytnúť nevyhnutný základ koherentného a jednotného uplatňovania opatrení na zvýšenie ochrany ECI, ako aj jasného vymedzenia príslušných povinností strán zainteresovaných na ECI. Dobrovoľné nezáväzné opatrenia by síce boli flexibilné, no nepredstavovali by potrebný stabilný základ, pretože by nebolo dostatočne jasné, kto čo robí, a takisto by neboli jasné práva a povinnosti strán zainteresovaných na ECI.

Postup identifikácie a označenia európskych kritických infraštruktúr a spoločný prístup k zhodnoteniu potreby zlepšiť ochranu týchto infraštruktúr možno stanoviť len prostredníctvom smernice, ktorá zabezpečí:

- primeranú úroveň ochrany v súvislosti s ECI,
- rovnaké práva a povinnosti pre všetky strany zainteresované na ECI,
- zachovanie stability vnútorného trhu.

Poškodenie alebo zničenie časti infraštruktúry v jednom členskom štáte môže mať nepriaznivý vplyv na niekoľko ďalších členských štátov a na európsku ekonomiku ako celok. Toto je čoraz pravdepodobnejšie, nakoľko nové technológie (napr. internet) a liberalizácia trhu (napr. pri dodávkach elektrickej energie a plynu) spôsobujú, že mnohé typy infraštruktúry sú súčasťou väčšej siete. Pri takýchto situáciách sú ochranné opatrenia silné len natoľko, ako ich najslabší článok. To znamená, že jednotná úroveň ochrany by mohla byť potrebná.

- **Sektorovo špecifický dialóg so zainteresovanými stranami**

Efektívna ochrana si vyžaduje komunikáciu, koordináciu a spoluprácu všetkých relevantných zainteresovaných strán, a to na vnútroštátnej úrovni, aj na úrovni EÚ.

Keďže väčšinu kritických infraštruktúr vlastní alebo prevádzkuje súkromný sektor, je dôležité, aby bol tento sektor plne zapojený. Každý prevádzkovateľ musí kontrolovať riadenie svojich rizík, pretože je to zvyčajne len on, kto rozhoduje o ochranných opatreniach a plánoch kontinuity činností. Plánovanie kontinuity činností by malo rešpektovať bežné podnikateľské postupy a logiku a ak je to možné, prijaté riešenia by sa mali zakladať na štandardných obchodných dohodách.

Sektory majú osobitné skúsenosti, odborné znalosti a požiadavky, pokiaľ ide o ochranu kritickej infraštruktúry.

Z tohto dôvodu a v súlade s odpoveďami na Zelenú knihu o EPCIP by mal prístup EÚ v plnej miere zahŕňať súkromný sektor, zohľadňujúc sektorové charakteristiky, a mal by vychádzať z existujúcich sektorovo špecifických ochranných opatrení.

- **Existujúce ustanovenia týkajúce sa návrhu**

Na úrovni EÚ v súčasnosti neexistujú žiadne horizontálne ustanovenia o kritickej infraštruktúre. Touto smernicou sa stanovuje postup identifikácie a označovania európskych

kritických infraštruktúr a spoločný prístup k zhodnoteniu potrieb zlepšiť ochranu týchto infraštruktúr.

Existuje mnoho sektorovo špecifických opatrení, medzi ktoré patria:

- v IT sektore:

  (a) smernica o univerzálnej službe (2002/22/ES), ktorá sa okrem iného týka integrity verejných elektronických komunikačných sietí,

  (b) smernica o povolení (2002/20/ES), ktorá sa okrem iného týka integrity verejných elektronických komunikačných sietí,

  (c) smernica o súkromí v elektronickej komunikácii (2002/58/ES), ktorá sa okrem iného týka bezpečnosti verejných elektronických komunikačných sietí,

  (d) rámcové rozhodnutie Rady 2005/222/SVV z 24. februára 2005 o útokoch na informačné systémy,

  (e) nariadenie (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií ENISA,

- v zdravotníckom sektore:

  (a) rozhodnutie Európskeho parlamentu a Rady č. 2119/98/ES z 24. septembra 1998, ktorým sa v Spoločenstve zriaďuje sieť na epidemiologický dohľad a kontrolu prenosných ochorení,

  (b) smernica Komisie 2003/94/ES z 8. októbra 2003, ktorou sa ustanovujú zásady a metodické pokyny správnej výrobnej praxe týkajúcej sa liekov na humánne použitie a skúšaných liekov na humánne použitie,

- vo finančnom sektore:

  (a) smernica Európskeho parlamentu a Rady 2004/39/ES z 21. apríla 2004 o trhoch s finančnými nástrojmi (MiFID),

  (b) štandardy pre dohľad nad retailovými platobnými systémami, ktoré prijala Rada guvernérov Európskej centrálnej banky (ECB) v júni 2003,

  (c) smernica 2006/48/ES Európskeho parlamentu a Rady z 14. júna 2006 o začatí a vykonávaní činností úverových inštitúcií,

  (d) smernica Európskeho parlamentu a Rady 2006/49/ES zo 14. júna 2006 o kapitálovej primeranosti investičných spoločností a úverových inštitúcií,

  (e) návrh smernice o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2000/12/ES a 2002/65/ES (KOM(2005) 603),

(f) smernica 2000/46/ES Európskeho parlamentu a Rady z 18. septembra 2000 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva,

(g) smernica Európskeho parlamentu a Rady 1998/26/ES z 19. mája 1998 o konečnom zúčtovaní v platobných systémoch,

- v sektore dopravy:

(a) nariadenie Európskeho parlamentu a Rady (ES) č. 725/2004 z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení,

(b) nariadenie Komisie (ES) č. 884/2005 z 10. júna 2005, ktorým sa ustanovujú postupy vykonávania inšpekcií Komisie v oblasti námornej bezpečnosti,

(c) smernica Európskeho parlamentu a Rady č. 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov,

(d) nariadenie Európskeho parlamentu a Rady (ES) č. 2320/2002 zo 16. decembra 2002 o ustanovení spoločných pravidiel v oblasti bezpečnostnej ochrany civilného letectva,

(e) nariadenie Komisie (ES) č. 622/2003 zo 4. apríla 2003 o ustanovení opatrení na vykonávanie spoločných základných noriem bezpečnostnej ochrany civilného letectva,

(f) nariadenie Komisie (ES) č. 1217/2003 zo 4. júla 2003, ktorým sa ustanovujú spoločné charakteristiky pre vnútroštátne programy kontroly kvality bezpečnosti civilného letectva,

(g) nariadenie Komisie (ES) č. 1486/2003 z 22. augusta 2003 ustanovujúce postupy pre vykonávanie inšpekcií Komisie v oblasti bezpečnostnej ochrany civilného letectva,

(h) nariadenie Komisie (ES) č. 68/2004 z 15. januára 2004, ktorým sa mení a dopĺňa nariadenie Komisie (ES) č. 622/2003 o ustanovení opatrení na vykonávanie spoločných základných noriem bezpečnostnej ochrany civilného letectva,

(i) nariadenie Európskeho parlamentu a Rady (ES) č. 849/2004 z 29. apríla 2004, ktorým sa mení a dopĺňa nariadenie (ES) č. 2320/2002 o ustanovení spoločných pravidiel v oblasti bezpečnostnej ochrany civilného letectva,

(j) nariadenie Komisie (ES) č. 1138/2004 z 21. júna 2004, ktorým sa stanovuje spoločná definícia citlivých častí ochranných priestorov na letiskách,

(k) nariadenie Komisie (ES) č. 781/2005 z 24. mája 2004, ktorým sa mení a dopĺňa nariadenie (ES) č. 622/2003 o ustanovení opatrení

na vykonávanie spoločných základných noriem bezpečnostnej ochrany civilného letectva,

(l) nariadenie Komisie (ES) č. 857/2005 zo 6. júna 2005, ktorým sa mení a dopĺňa nariadenie (ES) č. 622/2003 o ustanovení opatrení na vykonávanie spoločných základných noriem bezpečnostnej ochrany civilného letectva,

(m) smernica 2001/14/ES o prideľovaní kapacity železničnej infraštruktúry,

(n) preprava nebezpečného tovaru železničnou dopravou podlieha smernici 96/49/ES (zmenenej a doplnenej smernicou 2004/110/ES, ktorou sa prijal RID 2005)

(o) Dohovor o fyzickej ochrane jadrového materiálu (podpísaný v roku 1980, Euratom k nemu pristúpil v roku 1981 a platnosť nadobudol v roku 1987),

- v chemickom sektore:

(a) nebezpečné zariadenia podľa smernice Seveso II (smernica Rady 96/82/ES z 9. decembra 1996 o kontrole nebezpečenstiev veľkých havárií s prítomnosťou nebezpečných látok („smernica Seveso II“), zmenenej a doplnenej smernicou Európskeho parlamentu a Rady 2003/105/ES zo 16. decembra 2003,

- v jadrovom sektore:

(a) Smernica Rady 89/618/Euratom z 27. novembra 1989 o informovaní verejnosti o opatreniach na ochranu zdravia, ktoré sa majú uplatniť, a o krokoch, ktoré sa majú vykonať v prípade rádiologickej havarijnej situácie,

(b) Rozhodnutie Rady 87/600/Euratom zo 14. decembra 1987 o opatreniach Spoločenstva pre rýchlu výmenu informácií v prípade rádiologickej havarijnej situácie.

- **Súlad s inými politikami a cieľmi Únie**

Tento návrh je plne v súlade s cieľmi Únie a najmä s cieľom „zachovávať a rozvíjať Úniu ako priestor slobody, bezpečnosti a spravodlivosti, v ktorom je zaručený voľný pohyb osôb spolu s príslušnými opatreniami týkajúcimi sa ochrany vonkajších hraníc, azylu, prisťahovalectva a prevencie a boja proti zločinnosti“.

Tento návrh je v súlade s inými politikami, keďže nemá existujúce opatrenia nahradiť, ale len doplniť s cieľom zlepšiť ochranu ECI.

2) KONZULTÁCIE SO ZAINTERESOVANÝMI STRANAMI A POSÚDENIE VPLYVU

- **Konzultácie so zainteresovanými stranami**

Konzultácie týkajúce sa vývoja EPCIP sa uskutočnili so všetkými relevantnými zainteresovanými stranami, a to prostredníctvom:

- prijatia Zelenej knihy o EPCIP 17. novembra 2005, pričom obdobie konzultácií trvalo do 15. januára 2006. Oficiálne odpovede v rámci konzultácií poskytlo 22 členských štátov. K zelenej knihe sa taktiež vyjadrilo asi 100 predstaviteľov súkromného sektora. Odpovede vo všeobecnosti podporovali myšlienku vytvorenia EPCIP,

- Komisia usporiadala tri semináre o ochrane kritickej infraštruktúry (jún 2005, september 2005 a marec 2006). Na všetkých troch seminároch sa zúčastnili zástupcovia členských štátov. Zástupcovia súkromného sektora boli pozvaní na semináre, ktoré sa uskutočnili v septembri 2005 a marci 2006,

- neformálnych stretnutí kontaktných miest CIP. Komisia usporiadala pre kontaktné miesta CIP členských štátov dve stretnutia (v decembri 2005 a vo februári 2006),

- neformálnych stretnutí s predstaviteľmi súkromného sektora. Početné neformálne stretnutia sa uskutočnili so zástupcami niektorých súkromných podnikov, ako aj s priemyselnými združeniami,

- na internej úrovni Komisie pokračovala práca na vývoji EPCIP v rámci pravidelných stretnutí podskupiny pre ochranu kritickej infraštruktúry patriacej do medziútvarovej skupiny pre interné aspekty terorizmu.

- **Získavanie a využívanie odborných znalostí**

Potrebné odborné znalosti boli získané na početných stretnutiach a seminároch, ktoré sa uskutočnili v rokoch 2004, 2005 a 2006, ako aj počas procesu konzultácií v rámci Zelenej knihy o EPCIP. Zhromaždili sa informácie od všetkých relevantných zainteresovaných strán.

- **Hodnotenie vplyvu**

Kópia hodnotenia vplyvu EPCIP je pripojená.

3) PRÁVNE ASPEKTY NÁVRHU

- **Zhrnutie navrhovanej akcie**

Navrhnutá akcia tvorí horizontálny rámec pre identifikáciu a označovanie európskych kritických infraštruktúr a zhodnotenie potrieb zlepšiť ich ochranu.

- **Právny základ**

Právnym základom návrhu je článok 308 Zmluvy o založení Európskeho spoločenstva.

- **Princíp subsidiarity**

Princíp subsidiarity je dodržaný, pretože navrhované opatrenia nemožno uskutočniť na úrovni jednotlivých členských štátov EÚ, a preto musia byť prijaté na úrovni EÚ. Hoci je každý členský štát sám zodpovedný za ochranu kritickej infraštruktúry spadajúcej pod jeho jurisdikciu, z hľadiska bezpečnosti Európskej únie má rozhodujúci význam to, aby sa zaistila dostatočná ochrana infraštruktúry, ktorá má vplyv na dva alebo viac členských štátov alebo na jeden členský štát v prípade, že sa kritická infraštruktúra nachádza v inom členskom štáte, a aby sa žiadny členský štát nestal zraniteľným kvôli slabosti alebo nižším bezpečnostným štandardom iných členských štátov. Rovnaké pravidlá v oblasti bezpečnosti by zároveň pomohli zaistiť to, aby sa nenarušili pravidlá hospodárskej súťaže na vnútornom trhu.

- **Princíp proporcionality**

Návrh nejde nad rámec toho, čo je potrebné na dosiahnutie základného cieľa zvýšenia ochrany európskej kritickej infraštruktúry. Medzi najdôležitejšie myšlienky v návrhu patrí vytvorenie základného koordinačného mechanizmu na úrovni EÚ, uloženie povinnosti identifikovať svoje kritické infraštruktúry členským štátom, implementácia súboru základných bezpečnostných opatrení pre kritické infraštruktúry a napokon identifikácia a označenie európskych kritických infraštruktúr kľúčového významu. Návrh preto prináša minimálny počet požiadaviek, na ktorých základe je možné začať so zlepšovaním ochrany kritických infraštruktúr. Tento cieľ nemožno uspokojivo dosiahnuť prostredníctvom iných opatrení, ako je prijatie príslušných usmernení k EPCIP, pretože by sa tým nezabezpečila ani lepšia úroveň ochrany v rámci celej EÚ, ani plná účasť všetkých zainteresovaných strán.

- **Výber nástrojov**

Členské štáty majú rôzny prístup k ochrane kritickej infraštruktúry a rôzne právne systémy. Z týchto dôvodov je na vytvorenie spoločného postupu identifikácie a označovania európskych kritických infraštruktúr a spoločného prístupu k zhodnoteniu potreby zlepšiť ochranu týchto infraštruktúr najvhodnejším nástrojom smernica.

4) VPLYV NA ROZPOČET

Odhadovaný vplyv na rozpočet je v priloženom finančnom výkaze.

Program „Prevencia, pripravenosť a riadenie následkov terorizmu a ďalších rizík súvisiacich s bezpečnosťou“ na roky 2007 – 2013 prispeje k implementácii tejto smernice v oblasti ochrany ľudí proti bezpečnostným rizikám a ochrany tých fyzických zdrojov, služieb a informačno-technologických zariadení, sietí a infraštruktúr, ktorých narušenie alebo zničenie by vážne ovplyvnilo rozhodujúce funkcie spoločnosti, ako súčasť všeobecného programu nazvaného „Bezpečnosť a ochrana slobôd“.

Tento program sa neuplatňuje na záležitosti, ktoré patria do pôsobnosti iných finančných nástrojov, predovšetkým Nástroja rýchlej reakcie pri závažných núdzových situáciách, a Fondu solidarity EÚ.

5) ĎALŠIE INFORMÁCIE

- **Zrušenie existujúcich právnych predpisov**

Nie je potrebné zrušiť žiadne existujúce právne predpisy.

- **Podrobný výklad návrhu**

Článok 1 sa zaoberá predmetom smernice. V smernici sa stanovuje spoločný postup identifikácie a označenia európskych kritických infraštruktúr, t. j. tých infraštruktúr, ktorých zničenie alebo narušenie by ovplyvnilo dva alebo viaceré členské štáty alebo jeden členský štát v prípade, že sa kritická infraštruktúra nachádza v inom členskom štáte. Smernicou sa zároveň zavádza spoločný prístup k zhodnoteniu potreby zvýšiť ochranu európskych kritických infraštruktúr. Toto zhodnotenie pomôže pri príprave špecifických ochranných opatrení v jednotlivých sektoroch CIP.

Článok 2 – zoznam základných vymedzení pojmov predloženej smernice.

Článok 3 – upravuje postup identifikácie ECI. ECI predstavujú tie kritické infraštruktúry, ktorých narušenie alebo zničenie by významne ovplyvnilo dva alebo viaceré členské štáty alebo jeden členský štát v prípade, že sa kritická infraštruktúra nachádza v inom členskom štáte. Tento postup sa zakladá na trojstupňovom procese. Po prvé, Komisia spolu s členskými štátmi a relevantnými zainteresovanými stranami stanoví prierezové a sektorovo špecifické kritériá identifikácie ECI, ktoré sa potom prijmú v rámci postupu komitológie. Prierezové kritériá sa určujú podľa závažnosti narušenia alebo zničenia CI. Závažnosť dôsledkov narušenia alebo zničenia určitej infraštruktúry by sa mala v prípade potreby posudzovať na základe:

- vplyvu na verejnosť (počet ovplyvnených obyvateľov),
- ekonomických účinkov (závažnosť ekonomických strát a/alebo zhoršenie výrobkov alebo služieb),
- environmentálnych účinkov,
- politických účinkov,
- psychologických účinkov,
- dôsledkov na verejné zdravie.

Každý členský štát potom identifikuje tie infraštruktúry, ktoré spĺňajú kritériá. Nakoniec každý členský štát oznámi Komisii kritické infraštruktúry, ktoré spĺňajú stanovené kritériá. Príslušná činnosť sa vykonáva v prioritných sektoroch CIP, ktoré každoročne vyberá Komisia spomedzi tých, ktoré sú uvedené v prílohe I. Zoznam sektorov CIP v prílohe I sa môže meniť a dopĺňať prostredníctvom komitológie, pokiaľ sa tým nerozšíri rozsah pôsobnosti smernice. Zoznam sa teda môže meniť a dopĺňať predovšetkým s cieľom objasniť jeho obsah. Za prioritné sektory, v ktorých je potrebné okamžite konať, považuje Komisia sektory dopravy a energetiky.

Článok 4 – stanovuje postup označovania ECI. Po ukončení postupu identifikácie podľa článku 3 Komisia pripraví návrh zoznamu ECI. Návrh zoznamu vychádza z oznámení prijatých od členských štátov a iných relevantných informácií Komisie. Zoznam sa potom prijme v procese komitológie.

Článok 5 – bezpečnostné plány (OSP). Článok 5 požaduje od vlastníkov/prevádzkovateľov častí kritickej infraštruktúry označenej ako ECI, aby vypracovali OSP, ktorý identifikuje ich kritické európske infraštruktúry a stanovuje príslušné bezpečnostné riešenia na ich ochranu. Príloha 2 stanovuje, čo musia bezpečnostné plány prinajmenšom obsahovať:

- identifikáciu dôležitých kritických infraštruktúr,
- analýzu rizika založenú na scenároch najväčších hrozieb, zraniteľnosti jednotlivých infraštruktúr a možných účinkoch,
- identifikáciu, výber protiopatrení a postupov a stanovenie toho, ktoré z nich sú prioritné, s rozlišovaním medzi:
    - **stálymi bezpečnostnými opatreniami**, ktoré určujú nevyhnutné bezpečnostné investície a prostriedky, ktoré vlastník/prevádzkovateľ nedokáže zaistiť v krátkom čase. Patria sem informácie o všeobecných opatreniach, technických opatreniach (vrátane zavedenia detekčných systémov a prístupových kontrol, ochranných a preventívnych prostriedkov), organizačných opatreniach (vrátane postupov pre prípad poplachu a krízový manažment), kontrolných a overovacích opatreniach, komunikácii, zvyšovaní informovanosti a odbornej prípravy a bezpečnosti informačných systémov.
    - **odstupňovanými bezpečnostnými opatreniami**, ktoré by sa mohli uplatniť v závislosti od rôznych úrovní rizika a hrozieb.

Každý sektor CIP si môže vytvoriť sektorovo špecifické OSP založené na minimálnych požiadavkách prílohy II. Takéto sektorovo špecifické OSP možno prijať prostredníctvom komitológie.

Sektory, v ktorých už podobné povinnosti existujú, môžu byť podľa článku 5 ods. 2 oslobodené od povinností týkajúcich sa OSP na základe rozhodnutia prijatého v procese komitológie. Uznáva sa, že smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov už spĺňa požiadavky na vypracovanie bezpečnostného plánu.

Vypracovaný OSP by mal každý vlastník/prevádzkovateľ ECI predložiť príslušnému orgánu členského štátu. Každý členský štát vytvorí pre OSP kontrolný systém, ktorý vlastníkovi/prevádzkovateľovi ECI zaistí dostatočnú spätnú väzbu v súvislosti s kvalitou OSP, a najmä adekvátnosťou hodnotenia rizík a hrozieb.

Článok 6 – styčný úradník pre bezpečnosť (SLO). Článok 6 vyžaduje od všetkých vlastníkov/prevádzkovateľov CI označenej ako ECI, aby vymenovali styčného úradníka pre bezpečnosť. Tento SLO bude kontaktným miestom pre otázky bezpečnosti medzi ECI a príslušnými orgánmi CIP v členských štátoch. Bude preto dostávať všetky relevantné informácie týkajúce sa ochrany kritickej infraštruktúry od orgánov členských štátov a zároveň bude zodpovedný za poskytovanie príslušných informácií o ECI členskému štátu.

Článok 7 – podávanie správ. Článok 7 predkladá rad opatrení v oblasti podávania správ. Každý členský štát musí vykonať hodnotenia rizík a hrozieb vo vzťahu k ECI. Tieto informácie tvoria základ dialógu o otázkach bezpečnosti medzi členskými štátmi (kontrola) a ECI podľa článku 5. Keďže článok 5 vyžaduje od vlastníkov/prevádzkovateľov ECI, aby vypracovali bezpečnostné plány a predložili ich orgánom členského štátu, od každého členského štátu sa žiada, aby vypracoval všeobecný prehľad druhov zraniteľných miest, hrozieb a rizík v jednotlivých sektoroch CIP a aby uvedené informácie poskytol Komisii. Tieto informácie budú základom Komisiou vykonaného posúdenia, či sa majú vyžadovať ďalšie ochranné opatrenia. Informácie sa môžu neskôr použiť na vypracovanie posúdení vplyvu, ktoré sa budú prikladať k budúcim návrhom v tejto oblasti.

Tento článok tiež predpokladá rozvoj spoločných metód pre vykonávanie hodnotenia rizík, hrozieb a zraniteľnosti vzhľadom na kritické európske infraštruktúry. Takéto spoločné metódy by sa prijali v rámci postupu komitológie.

Článok 8 – Podpora ECI zo strany Komisie. Komisia podporí vlastníkov/prevádzkovateľov ECI umožnením prístupu k dostupným osvedčeným postupom a metódam týkajúcim sa CIP. Komisia začne zhromažďovať uvedené informácie z rôznych zdrojov (napr. z členských štátov, vlastných prác) a sprístupní ich dotknutým osobám.

Článok 9 – kontaktné miesta CIP. S cieľom zabezpečiť spoluprácu a koordináciu otázok CIP musí každý členský štát ustanoviť kontaktné miesto CIP. Kontaktné miesto by koordinovalo záležitosti CIP v rámci členského štátu, s inými členskými štátmi a s Komisiou.

Článok 10 – Dôvernosť a výmena informácií súvisiacich s CIP. Dôvernosť a výmena informácií súvisiacich s CIP je kľúčovým a zároveň citlivým prvkom práce v oblasti CIP. Preto smernica požaduje od Komisie a členských štátov, aby prijali primerané opatrenia na ochranu informácií. Všetci členovia personálu, ktorí prichádzajú do styku s utajenými informáciami o CIP, musia prejsť nevyhnutnou bezpečnostnou previerkou, ktorú vykonávajú orgány členského štátu.

Článok 11 – Výbor. Niektoré prvky smernice sa implementujú prostredníctvom komitológie. Výbor bude zložený z kontaktných miest CIP. Na účely článku 5 ods. 2, t. j. na oslobodenie niektorých sektorov od povinnosti vypracovať OSP, sa bude používať konzultačný postup.

Regulačný postup sa predpokladá v nasledujúcich otázkach:

- článok 3 ods. 1 – prijatie prierezových a sektorovo špecifických kritérií na identifikáciu ECI,
- článok 3 ods. 2 – mení a dopĺňa zoznam sektorov CIP v prílohe 1,
- článok 4 ods. 2 – prijatie návrhu zoznamu ECI,
- článok 5 ods. 2 – vypracovanie sektorovo špecifických požiadaviek na bezpečnostné plány,
- článok 7 ods. 2 – vypracovanie spoločnej predlohy pre všeobecné správy o identifikovaných rizikách, hrozbách a zraniteľných miestach,

- článok 7 ods. 4 – vypracovanie spoločných metód pre vykonávanie hodnotení rizík, hrozieb a zraniteľnosti.

2006/0276 (CNS)

Návrh

SMERNICA RADY

o identifikácii a označení európskej kritickej infraštruktúry a zhodnotení potreby zlepšiť jej ochranu

(Text s významom pre EHP)

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 308,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 203,

so zreteľom na návrh Komisie[1],

so zreteľom na stanovisko Európskeho parlamentu[2],

so zreteľom na stanovisko Európskej centrálnej banky[3],

keďže:

(1) V júni 2004 požiadala Európska rada o prípravu všeobecnej stratégie na ochranu kritických infraštruktúr[4]. V nadväznosti na to Komisia 20. októbra 2004 prijala Oznámenie o ochrane najdôležitejšej infraštruktúry v boji proti terorizmu[5], v ktorom predložila návrhy možných opatrení na zvýšenie úrovne európskej prevencie teroristických útokov proti kritickej infraštruktúre, pripravenosti a reakcie na ne.

(2) Dňa 17. novembra 2005 Komisia prijala Zelenú knihu o Európskom programe na ochranu najdôležitejšej infraštruktúry[6], v ktorej predstavila možné scenáre uskutočnenia programu a Varovnej informačnej siete kritickej infraštruktúry (CIWIN). Odpovede, ktoré získala v súvislosti so zelenou knihou, jasne poukázali na nevyhnutnosť vytvorenia rámca Spoločenstva týkajúceho sa ochrany kritickej infraštruktúry. Uznala sa potreba zvýšenia schopnosti ochrany kritickej infraštruktúry v Európe a zníženia zraniteľnosti týchto infraštruktúr. Zdôraznil sa význam princípu subsidiarity a dialógu so zainteresovanými stranami.

---

1 Ú. v. EÚ C […], […], s. […].
2 Ú. v. EÚ C […], […], s. […].
3 Ú. v. EÚ C […], […], s. […].
4 Dokument Rady 10679/2/04 REV 2.
5 KOM(2004) 702.
6 KOM(2005) 576.

(3) V decembri 2005 Rada pre spravodlivosť a vnútorné záležitosti požiadala Komisiu, aby predložila návrh Európskeho programu na ochranu najdôležitejšej infraštruktúry (EPCIP) a rozhodla, že by mal byť založený na prístupe, ktorý by pokrýval nebezpečenstvá každého druhu a ktorý by prednostne čelil hrozbám plynúcim z terorizmu. Tento prístup by v procese ochrany kritickej infraštruktúry zohľadňoval človekom spôsobené a technologické hrozby a prírodné katastrofy, ale prioritou by bola hrozba terorizmu. Ak sa v sektore kritickej infraštruktúry považuje úroveň ochranných opatrení za adekvátnu vo vzťahu k obzvlášť vážnej hrozbe, zainteresované strany by sa mali sústrediť na iné hrozby, voči ktorým sú stále zraniteľné.

(4) Primárnu zodpovednosť za ochranu kritických infraštruktúr v súčasnosti nesú členské štáty a vlastníci/prevádzkovatelia kritických infraštruktúr. Toto by sa nemalo zmeniť.

(5) V Spoločenstve existuje určitý počet kritických infraštruktúr, ktorých narušenie alebo zničenie by ovplyvnilo dva alebo viaceré členské štáty alebo iný členský štát ako je štát, v ktorom sa nachádza kritická infraštruktúra. Toto môže zahŕňať cezhraničné medzisektorové účinky vyplývajúce zo závislostí medzi vzájomne prepojenými infraštruktúrami. Uvedené európske kritické infraštruktúry by sa mali identifikovať a označiť podľa spoločného postupu. Potreba zvýšenia ochrany takýchto kritických infraštruktúr by sa mala hodnotiť na základe spoločného rámca. Bilaterálne schémy spolupráce medzi členskými štátmi v oblasti ochrany kritickej infraštruktúry predstavujú osvedčený a účinný prostriedok na ochranu cezhraničnej kritickej infraštruktúry. EPCIP by mal z takejto spolupráce vychádzať.

(6) Keďže existujú rôzne sektory s osobitnými skúsenosťami, odbornými znalosťami a požiadavkami v súvislosti s ochranou kritickej infraštruktúry, mal by sa vytvoriť a implementovať prístup k ochrane kritickej infraštruktúry na úrovni Spoločenstva, ktorý by zohľadňoval špecifiká sektorov a existujúce sektorovo špecifické opatrenia, vrátane tých, ktoré už existujú na úrovni EÚ, na národnej a regionálnej úrovni a v prípade potreby vrátane cezhraničných dohôd o vzájomnej pomoci medzi vlastníkmi/prevádzkovateľmi už existujúcej kritickej infraštruktúry. Vzhľadom na veľmi dôležitú úlohu súkromného sektora pri kontrole a riadení rizika, plánovaní kontinuity činností a obnove po katastrofách, bude musieť prístup Spoločenstva podporovať plné zapojenie súkromného sektora. Vypracovanie spoločného zoznamu sektorov kritickej infraštruktúry je nevyhnutné na to, aby sa uľahčilo presadenie sektorovo špecifického prístupu k ochrane kritickej infraštruktúry.

(7) Každý vlastník/prevádzkovateľ európskej kritickej infraštruktúry by mal vypracovať bezpečnostný plán, v ktorom by identifikoval kritické infraštruktúry a uviedol príslušné bezpečnostné riešenia na ich ochranu. V bezpečnostnom pláne by sa mali brať do úvahy hodnotenia zraniteľnosti, hrozieb a rizík, ako aj iné relevantné informácie poskytnuté orgánmi členských štátov.

(8) Každý vlastník/prevádzkovateľ európskej kritickej infraštruktúry by mal menovať styčného úradníka pre bezpečnosť, aby sa tak uľahčila spolupráca a komunikácia s príslušnými vnútroštátnymi orgánmi pre ochranu kritickej infraštruktúry.

(9) Účinná identifikácia rizík, hrozieb a zraniteľných miest v niektorých sektoroch vyžaduje komunikáciu medzi vlastníkmi/prevádzkovateľmi európskej kritickej infraštruktúry a členskými štátmi, aj medzi členskými štátmi a Komisiou. Každý členský štát by mal zhromažďovať informácie týkajúce sa európskych kritických

infraštruktúr, ktoré sa nachádzajú na jeho území. Komisia by mala od členských štátov dostávať všeobecné informácie o zraniteľných miestach, hrozbách a rizikách, v prípade potreby vrátane informácií o možných nedostatkoch a závislostiach medzi sektormi, ktoré by prípadne mohli byť základom pre rozpracovanie špecifických návrhov na zvýšenie ochrany ECI.

(10) S cieľom uľahčiť zvýšenie ochrany európskych kritických infraštruktúr by sa mala vypracovať metodológia identifikácie a klasifikácie zraniteľných miest, hrozieb a rizík, ktoré vznikajú vo vzťahu k týmto infraštruktúram.

(11) Len spoločný rámec môže tvoriť nevyhnutný základ koherentnej implementácie opatrení na ochranu európskej kritickej infraštruktúry a jasne definovať príslušné povinnosti všetkých relevantných zainteresovaných strán. Vlastníci/prevádzkovatelia európskej kritickej infraštruktúry by mali mať prístup k osvedčeným postupom a metódam ochrany kritickej infraštruktúry.

(12) Účinná ochrana kritickej infraštruktúry vyžaduje komunikáciu, koordináciu a spoluprácu na vnútroštátnej úrovni aj na úrovni Spoločenstva. Toto sa dá najlepšie dosiahnuť formou ustanovenia kontaktných miest CIP v každom členskom štáte, ktoré by mali koordinovať záležitosti CIP na internej úrovni, ako aj s inými členskými štátmi a Komisiou.

(13) S cieľom rozvinúť činnosti ochrany kritickej infraštruktúry v oblastiach, ktoré si vyžadujú stupeň dôvernosti, je vhodné zabezpečiť koherentnú a bezpečnú výmenu informácií v rámci tejto smernice. Niektoré informácie o ochrane kritickej infraštruktúry sú takej povahy, že ich zverejnenie by ohrozilo ochranu verejného záujmu pokiaľ ide o verejnú bezpečnosť. Určité informácie o kritických infraštruktúrach, ktoré by mohli byť zneužité na naplánovanie alebo vykonanie takej činnosti, ktorá by mala neprijateľné dôsledky pre kritickú infraštruktúru, by sa teda mali utajiť a prístup k nim by sa mal udeliť len na základe potreby vedomosti o nich, a to na úrovni Spoločenstva aj na úrovni členských štátov.

(14) Výmena informácií o kritickej infraštruktúre by sa mala uskutočňovať v atmosfére dôvery a istoty. Výmena informácií si vyžaduje vzťah dôvery, aby tak dotknuté spoločnosti a organizácie vedeli, že ich citlivé údaje sú dostatočne chránené. S cieľom podporiť uvedenú výmenu informácií by sa malo podnikom vysvetliť, že výhody poskytnutia informácií súvisiacich s kritickou infraštruktúrou prevažujú nad nákladmi, ktoré tým priemyslu a spoločnosti všeobecne vznikajú. Výmena informácií o ochrane kritickej infraštruktúry by sa preto mala podporiť.

(15) Táto smernica dopĺňa existujúce sektorovo špecifické opatrenia na úrovni Spoločenstva a v členských štátoch. Existujúce mechanizmy Spoločenstva by sa mali naďalej používať a mali by napomôcť celkovej implementácii tejto smernice.

(16) Opatrenia nevyhnutné na vykonanie tejto smernice by sa mali prijať v súlade s rozhodnutím Rady 1999/468/ES z 28. júna 1999, ktorým sa ustanovujú postupy pre výkon vykonávacích právomocí prenesených na Komisiu[7].

---

[7] Ú. v. ES L 184, 17.7.1999, s. 23.

(17) Keďže ciele tejto smernice, a to vytvorenie postupu identifikácie a označovania európskych kritických infraštruktúr a zavedenie spoločného prístupu k zhodnoteniu potrieb zvýšenia ochrany takýchto infraštruktúr, nemôžu členské štáty uspokojivo dosiahnuť sami a z dôvodov rozsahu tejto činnosti ich možno lepšie dosiahnuť na úrovni Spoločenstva, Spoločenstvo môže prijať opatrenia v súlade s princípom subsidiarity podľa článku 5 Zmluvy. V súlade s princípom proporcionality podľa uvedeného článku neprekračuje táto smernica rámec nevyhnutný na dosiahnutie uvedených cieľov.

(18) Touto smernicou sa rešpektujú základné práva a dodržiavajú zásady uznávané najmä Chartou základných práv Európskej únie.

PRIJALA TÚTO SMERNICU:

Článok 1
Predmet

Touto smernicou sa stanovuje postup identifikácie a označenia európskych kritických infraštruktúr a spoločný prístup k zhodnoteniu potrieb zlepšiť ochranu týchto infraštruktúr.

Článok 2
Vymedzenie pojmov

Na účely tejto smernice:

a) „kritická infraštruktúra“ – infraštruktúry alebo ich časti, ktoré majú zásadný význam z hľadiska zachovania dôležitých funkcií spoločnosti, vrátane zásobovacieho reťazca, zdravia, bezpečnosti, istoty, hospodárskeho a sociálneho blahobytu osôb,

b) „európska kritická infraštruktúra” – kritické infraštruktúry, ktorých narušenie alebo zničenie by významne ovplyvnilo dva alebo viaceré členské štáty alebo jeden členský štát v prípade, že sa kritická infraštruktúra nachádza v inom členskom štáte. Toto zahŕňa účinky vyplývajúce zo závislostí medzi sektormi na iné typy infraštruktúry,

c) „závažnosť“ – vplyv narušenia alebo zničenia určitej infraštruktúry, najmä so zreteľom na:

- vplyv na verejnosť (počet ovplyvnených obyvateľov),
- ekonomické účinky (závažnosť ekonomických strát a/alebo zhoršenie výrobkov alebo služieb),
- environmentálne účinky,
- politické účinky,
- psychologické účinky,
- dôsledky na verejné zdravie,

d) „zraniteľnosť“ – vlastnosť základného prvku koncepcie, realizácie alebo fungovania kritickej infraštruktúry, ktorá ju robí náchylnou na narušenie alebo zničenie hrozbou a zahŕňa závislosti na iných typoch infraštruktúry,

e) „hrozba“ – akékoľvek náznaky, okolnosti alebo udalosti, ktoré môžu narušiť alebo zničiť kritickú infraštruktúru alebo niektorý jej prvok,

f) „riziko“ – možnosť straty, zničenia alebo poškodenia so zreteľom na hodnotu, ktorú vlastník/prevádzkovateľ pripisuje danej infraštruktúre, a vplyv straty alebo zmeny infraštruktúry a pravdepodobnosť, že určité zraniteľné miesto bude využité prostredníctvom konkrétnej hrozby,

g) „informácie o ochrane kritickej infraštruktúry“ – špecifické skutočnosti o kritickej infraštruktúre, ktoré by v prípade zverejnenia mohli byť zneužité na naplánovanie a vykonanie takej činnosti, ktorá by spôsobila výpadok kritickej infraštruktúry alebo by mala neprijateľné dôsledky pre kritickú infraštruktúru.

Článok 3
Identifikácia európskej kritickej infraštruktúry

1. Prierezové a sektorovo špecifické kritériá, ktoré sa majú použiť na identifikáciu európskych kritických infraštruktúr sa prijmú v súlade s postupom uvedeným v článku 11 ods. 3. Môžu sa zmeniť a doplniť v súlade s postupom uvedeným v článku 11 ods. 3.

   Pri vypracúvaní prierezových kritérií, ktoré sa horizontálne uplatňujú na všetky sektory kritickej infraštruktúry, sa zohľadní závažnosť účinku narušenia alebo zničenia určitej infraštruktúry. Budú prijaté najneskôr do [*jedného roka po nadobudnutí účinnosti tejto smernice*].

   Sektorovo špecifické kritériá sa vypracujú pre prioritné sektory, pričom sa zoberú do úvahy charakteristiky jednotlivých sektorov kritickej infraštruktúry a ak to je vhodné, zapoja sa relevantné zainteresované strany. Prijmú sa pre každý prioritný sektor najneskôr do jedného roka po označení sektora za prioritný.

2. Prioritné sektory, ktoré sa majú použiť na účely vypracovania kritérií ustanovených v odseku 1, každoročne určuje Komisia spomedzi tých, ktoré sú uvedené v prílohe 1.

   Prílohu 1 možno zmeniť a doplniť v súlade s postupom uvedeným v článku 11 ods. 3, pokiaľ sa tým nerozširuje rozsah pôsobnosti tejto smernice.

3. Každý členský štát identifikuje kritické infraštruktúry, ktoré sa nachádzajú na jeho území, ako aj kritické infraštruktúry mimo jeho územia, ktoré ho môžu ovplyvniť, ktoré spĺňajú kritériá prijaté podľa odsekov 1 a 2.

   Každý členský štát oznámi Komisii takto identifikované kritické infraštruktúry najneskôr jeden rok po prijatí príslušných kritérií a potom priebežne.

Článok 4
Označenie európskej kritickej infraštruktúry

1. Na základe oznámení podľa druhého pododseku článku 3 ods. 3 a akýchkoľvek iných informácií, ktoré má k dispozícii, Komisia navrhne zoznam kritických infraštruktúr, ktoré sa majú označiť ako európske kritické infraštruktúry.

2. Zoznam kritických infraštruktúr označených ako európska kritická infraštruktúra sa prijme v súlade s postupom uvedeným v článku 11 ods. 3.

   Zoznam sa môže zmeniť a doplniť v súlade s postupom uvedeným v článku 11 ods. 3.

Článok 5
Bezpečnostné plány

1. Každý členský štát uloží vlastníkom/prevádzkovateľom všetkých európskych kritických infraštruktúr na svojom území povinnosť vypracovať a aktualizovať bezpečnostný plán a revidovať ho prinajmenšom každé dva roky.

2. V bezpečnostnom pláne sa určia časti európskej kritickej infraštruktúry a stanovia príslušné bezpečnostné opatrenia na ich ochranu v súlade s prílohou II. V súlade s postupom uvedeným v článku 11 ods. 3 možno prijať sektorovo špecifické požiadavky týkajúce sa bezpečnostného plánu, ktoré zohľadňujú existujúce opatrenia Spoločenstva.

   Komisia môže v súlade s postupom podľa článku 11 ods. 2 rozhodnúť, že dodržiavanie opatrení uplatniteľných na špecifické sektory uvedené v prílohe 1 spĺňa požiadavku na vytvorenie a aktualizáciu bezpečnostného plánu.

3. Vlastník/prevádzkovateľ európskej kritickej infraštruktúry predloží bezpečnostný plán príslušnému orgánu členského štátu v priebehu jedného roka po označení kritickej infraštruktúry za kritickú európsku infraštruktúru.

   Ak sa na základe odseku 2 prijmú sektorovo špecifické požiadavky týkajúce sa bezpečnostného plánu, predloží sa tento bezpečnostný plán príslušnému orgánu členského štátu v priebehu jedného roka po prijatí sektorovo špecifických požiadaviek.

4. Každý členský štát vytvorí systém zabezpečujúci adekvátnu a pravidelnú kontrolu bezpečnostných plánov a ich implementácie na základe hodnotení rizík a hrozieb vykonaných podľa článku 7 ods. 1.

5. Súlad so smernicou Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov spĺňa požiadavku na vypracovanie bezpečnostného plánu.

Článok 6
Styční úradníci pre bezpečnosť

1. Každý členský štát bude od vlastníkov/prevádzkovateľov európskych kritických infraštruktúr nachádzajúcich sa na jeho území vyžadovať, aby vymenovali styčného úradníka pre bezpečnosť ako kontaktné miesto pre otázky týkajúce sa bezpečnosti medzi vlastníkom/prevádzkovateľom infraštruktúry a príslušnými orgánmi na ochranu kritickej infraštruktúry v členskom štáte. Styčný úradník pre bezpečnosť bude vymenovaný v priebehu jedného roka po označení kritickej infraštruktúry ako európskej kritickej infraštruktúry.

2. Každý členský štát oznámi relevantné informácie o identifikovaných rizikách a hrozbách styčným úradníkom pre bezpečnosť dotknutej európskej kritickej infraštruktúry.

Článok 7
Podávanie správ

1. Každý členský štát vykoná hodnotenia rizík a hrozieb vo vzťahu ku kritickej európskej infraštruktúre, ktorá sa nachádza na jeho území, v lehote jedného roka od označenia kritickej infraštruktúry ako ECI.

2. Každý členský štát podáva Komisii súhrnné správy o druhoch zraniteľných miest, hrozieb a rizík v jednotlivých sektoroch uvedených v prílohe 1 v lehote 18 mesiacov po prijatí zoznamu ustanoveného v článku 4 ods. 2 a potom priebežne každé dva roky.

   Pre tieto správy sa v súlade s postupom uvedeným v článku 11 ods. 3 vypracuje spoločný vzor.

3. Komisia pre každý jednotlivý sektor posúdi, či sú na ochranu európskych kritických infraštruktúr potrebné špecifické ochranné opatrenia.

4. Spoločné metódy vykonávania hodnotení zraniteľnosti, hrozieb a rizík, vzhľadom na európske kritické infraštruktúry možno podľa jednotlivých sektorov vypracovať v súlade s postupom uvedeným v článku 11 ods. 3.

Článok 8
Podpora ECI zo strany Komisie

Komisia podporuje vlastníkov/prevádzkovateľov označených európskych kritických infraštruktúr tak, že im umožní prístup k dostupným osvedčeným postupom a metódam týkajúcim sa ochrany kritickej infraštruktúry.

Článok 9
Kontaktné miesta CIP

1. Každý členský štát ustanoví kontaktné miesto ochrany kritickej infraštruktúry.

2. Kontaktné miesto koordinuje záležitosti ochrany kritickej infraštruktúry v rámci členského štátu, s inými členskými štátmi a s Komisiou.

Článok 10
Dôvernosť a výmena informácií súvisiacich s CIP

1. Pri uplatňovaní tejto smernice prijme Komisia v súlade s rozhodnutím 2001/844/ES, ESUO, Euratom primerané opatrenia na ochranu informácií dôvernej povahy, ku ktorým má prístup alebo ktoré jej oznámia členské štáty. Členské štáty prijmú rovnocenné opatrenia v súlade s príslušnými vnútroštátnymi právnymi predpismi. Pritom je potrebné zohľadniť závažnosť možného vplyvu na základné záujmy Spoločenstva alebo jedného či viacerých členských štátov.

2. Každá osoba, ktorá podľa tejto smernice v mene členského štátu prichádza do styku s dôvernými informáciami, musí prejsť bezpečnostnou previerkou primeraného stupňa, ktorú vykonáva dotknutý členský štát.

3. Členské štáty zabezpečia, aby sa informácie o ochrane kritickej infraštruktúry predložené členským štátom alebo Komisii nezneužili na iné účely ako je ochrana kritickej infraštruktúry.

Článok 11
Výbor

1. Komisii pomáha výbor zložený z jedného zástupcu za každé kontaktné miesto CIP.

2. Ak sa odkazuje na tento odsek, uplatňujú sa články 3 a 7 rozhodnutia 1999/468/ES so zreteľom na ustanovenia článku 8 tohto nariadenia.

3. Ak sa odkazuje na tento odsek, uplatňujú sa články 5 a 7 rozhodnutia 1999/468/ES so zreteľom na ustanovenia článku 8 uvedeného rozhodnutia.

   Obdobie stanovené v článku 5 ods. 6 rozhodnutia 1999/468/ES sa stanovuje na jeden mesiac.

4. Výbor prijme svoj rokovací poriadok.

Článok 12
Implementácia

1. Členské štáty najneskôr do 31. decembra 2007 uvedú do platnosti zákony, iné právne predpisy a správne opatrenia, potrebné na dosiahnutie súladu s touto smernicou. Komisii bezodkladne oznámia znenie týchto ustanovení a tabuľku zhody medzi týmito ustanoveniami a touto smernicou.

   Keď členské štáty prijmú tieto ustanovenia, budú obsahovať odkaz na túto smernicu alebo bude takýto odkaz uvedený pri ich úradnom uverejnení. Podrobnosti o odkaze upravia členské štáty.

2. Členské štáty oznámia Komisii znenia hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice.

Článok 13
Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 14
Adresáti

Táto smernica je určená všetkým členským štátom.

V Bruseli

Za Radu

PRÍLOHA I

ZOZNAM SEKTOROV KRITICKEJ INFRAŠTRUKTÚRY

Sektor		Podsektor	
I	Energia	1	Ťažba ropy a zemného plynu, rafinovanie, úprava, skladovanie a distribúcia potrubiami
		2	Výroba a prenos elektrickej energie
II	Jadrový priemysel	3	Výroba a skladovanie/spracúvanie jadrového materiálu
III	Informačné, komunikačné technológie, IKT	4	Ochrana informačného systému a siete
		5	Automatizácia prístrojového vybavenia a kontrolné systémy (SCADA atď.)
		6	Internet
		7	Poskytovanie pevnej telekomunikačnej siete
		8	Poskytovanie mobilnej telekomunikačnej siete
		9	Rádiová komunikácia a navigácia
		10	Satelitná komunikácia
		11	Rozhlasové vysielanie
IV	Voda	12	Zabezpečenie pitnej vody
		13	Kontrola kvality vody
		14	Zadržiavanie vody a kontrola množstva vody
V	Potraviny	15	Zabezpečenie potravín a ich bezpečnosti a nezávadnosti
VI	Zdravie	16	Lekárska a nemocničná starostlivosť
		17	Lieky, séra, vakcíny a farmaceutické výrobky
		18	Biologické laboratóriá a biologické účinné látky
VII	Finančný sektor	19	Infraštruktúry a systémy platieb a zúčtovania a vyrovnania cenných papierov
		20	Regulované trhy
VIII	Doprava	21	Cestná doprava
		22	Železničná doprava
		23	Letecká doprava
		24	Vnútrozemská vodná doprava
		25	Námorná doprava na dlhé a krátke vzdialenosti
IX	Chemický priemysel	26	Výroba a skladovanie/spracúvanie chemických látok
		27	Potrubia s nebezpečným tovarom (chemické látky)
X	Vesmír	28	Vesmír
XI	Výskumné zariadenia	29	Výskumné zariadenia

PRÍLOHA II

BEZPEČNOSTNÝ PLÁN (OSP)

V bezpečnostnom pláne sa identifikuje kritická infraštruktúra vlastníkov/prevádzkovateľov a stanovujú príslušné bezpečnostné riešenia na ich ochranu. OSP bude prinajmenšom zahŕňať:

– identifikáciu dôležitých častí kritických infraštruktúr,

– analýzu rizík založenú na scenároch najväčších hrozieb, zraniteľnosti jednotlivých častí infraštruktúr a možných účinkoch,

– identifikáciu, výber protiopatrení a postupov a stanovenie toho, ktoré z nich sú prioritné, s rozlišovaním medzi:

- **stálymi bezpečnostnými opatreniami**, ktoré určujú nevyhnutné bezpečnostné investície a prostriedky, ktoré vlastník/prevádzkovateľ nedokáže zaistiť v krátkom čase. Patria sem informácie o všeobecných opatreniach, technických opatreniach (vrátane zavedenia detekčných systémov a prístupových kontrol, ochranných a preventívnych prostriedkov), organizačných opatreniach (vrátane postupov pre prípad poplachu a krízový manažment), kontrolných a overovacích opatreniach, komunikácii, zvyšovaní informovanosti a odbornej prípravy a bezpečnosti informačných systémov.

- **odstupňovanými bezpečnostnými opatreniami**, ktoré by sa mohli uplatniť v závislosti od rôznych úrovní rizika a hrozieb.

LEGISLATÍVNY FINANČNÝ VÝKAZ

Oblasť(-ti) politiky: Spravodlivosť a vnútorné záležitosti

Činnosť: Ochrana kritickej infraštruktúry

NÁZOV AKCIE: Smernica Rady o identifikovaní a označení európskej kritickej infraštruktúry a hodnotení potreby zlepšenia jej ochrany

1. ROZPOČTOVÉ POLOŽKY + VÝDAVKOVÉ KAPITOLY

neuv.

2. CELKOVÉ ČÍSELNÉ ÚDAJE

2.1. Celkové pridelené prostriedky na akciu (časť B): v miliónoch EUR na viazané rozpočtové prostriedky

neuv.

2.2. Obdobie uplatňovania:

Začiatok roku 2006

2.3. Celkový viacročný odhad výdavkov:

a) Zhrnutie viazaných rozpočtových prostriedkov a platobných rozpočtových prostriedkov (finančná intervencia) (*pozri bod 6.1.1*)

v miliónoch EUR (*zaokrúhlené na 3 desatinné miesta*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Celkove
Viazané rozpočtové prostriedky	-	-	-	-	-	-	-
Platobné rozpočtové prostriedky	-	-	-	-	-	-	-

b) Technická a administratívna pomoc a podporné výdavky (*pozri bod 6.1.2*)

Viazané rozpočtové prostriedky	-	-	-	-	-	-	-
Platobné rozpočtové prostriedky	-	-	-	-	-	-	-

Medzisúčet a+b	-	-	-	-	-	-	-

Viazané rozpočtové prostriedky	-	-	-	-	-	-	-
Platobné rozpočtové prostriedky	-	-	-	-	-	-	-

c) Celkový finančný vplyv výdavkov na ľudské zdroje a iných administratívnych výdavkov *(pozri body 7.2 a 7.3)*

Viazané rozpočtové prostriedky/platobné rozpočtové prostriedky	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000

SPOLU a+b+c	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000
Viazané rozpočtové prostriedky	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000
Platobné rozpočtové prostriedky	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000

2.4. Zlučiteľnosť s finančným plánovaním a finančným výhľadom

Smernica je zlučiteľná s programom Prevencia, pripravenosť a riadenie následkov terorizmu a ďalších rizík súvisiacich s bezpečnosťou na roky 2007 – 2013.

2.5. Finančný vplyv na príjmy:

Nedávno prijatý program „Prevencia, pripravenosť a riadenie následkov terorizmu a ďalších rizík súvisiacich s bezpečnosťou“ na roky 2007 – 2013 (137,5 mil. EUR) prispeje k implementácii EPCIP v oblasti bezpečnostných rizík a tých fyzických zdrojov, služieb, informačno-technologických zariadení, sietí a infraštruktúr, ktorých narušenie alebo zničenie by mohlo vážne ovplyvniť dôležité funkcie spoločnosti, ako súčasť všeobecného programu „Bezpečnosť a ochrana slobôd“. Rozsah pôsobnosti programu je obmedzený, pretože sa nevzťahuje na investície súvisiace s hardvérom alebo vybavením. Tento program sa neuplatňuje na záležitosti, ktoré patria do pôsobnosti iných finančných nástrojov, a predovšetkým Nástroja rýchlej reakcie pri závažných núdzových situáciách.

V oblasti predchádzania a pripravenosti sa program zameriava na:

a) podnecovanie k hodnoteniu hrozieb a rizík vznikajúcich v súvislosti s kritickou infraštruktúrou, vrátane hodnotenia na mieste, jeho presadzovanie a podporu, s cieľom určiť hrozby a zraniteľné miesta, ako aj potreby na zvýšenie ich bezpečnosti,

b) presadzovanie a podporu spoločných operatívnych opatrení na zvýšenie bezpečnosti cezhraničných zásobovacích reťazcov za predpokladu, že sa tým nenarušia pravidlá hospodárskej súťaže na vnútornom trhu,

c) presadzovanie a podporu rozvoja minimálnych bezpečnostných štandardov, výmeny osvedčených postupov, nástrojov hodnotenia rizík, metodológie na porovnávanie infraštruktúr v rôznych sektoroch a stanovenie priorít, analýzy

zraniteľných miest a vzájomných závislostí pri ochrane kritických infraštruktúr,

d) presadzovanie a podporu koordinácie a spolupráce v oblasti ochrany kritickej infraštruktúry na úrovni Spoločenstva. Ak je to potrebné, vypracovanie návrhov na minimálne ochranné opatrenia a spoločné usmernenia.

V oblasti riadenia následkov sa program zameriava na:

a) podnecovanie k výmene know-how, skúseností a technológie, presadzovanie a podporu tejto výmeny,

b) podnecovanie k rozvoju príslušnej metodológie a pohotovostných plánov, jeho presadzovanie a podpora,

c) zabezpečenie včasného sprístupnenia špecifických odborných znalostí v oblasti bezpečnosti v rámci celkového krízového manažmentu, mechanizmu včasného varovania a civilnej ochrany.

Návrh preto nemá žiadny finančný vplyv na príjmy.

3. ROZPOČTOVÉ CHARAKTERISTIKY

Druh výdavkov		**Nové**	**Príspevok EZVO**	**Príspevky kandidátskych krajín**	**Výdavková kapitola vo finančnom výhľade**
Nepovinné	Nedif.	neuv.	neuv.	neuv.	**Nie** neuv.

4. PRÁVNY ZÁKLAD

Právnym základom návrhu je článok 308 Zmluvy o založení Európskeho spoločenstva.

5. OPIS A ZDÔVODNENIE

5.1. Potreba intervencie zo strany Spoločenstva

5.1.1. Sledované ciele

Členské štáty majú rôzny prístup k ochrane kritickej infraštruktúry a rôzne právne predpisy, preto je na vytvorenie spoločného rámca EPCIP najvhodnejším nástrojom smernica. Navrhnutím niekoľkých kľúčových myšlienok a umožnením toho, aby členské štáty použili prístupy, ktoré najviac zodpovedajú ich potrebám, možno dosiahnuť ciele EPCIP v plnej miere, pričom sa bude stavať na tom, čo už bolo dosiahnuté.

5.1.2. Opatrenia prijaté v súvislosti s hodnotením ex ante

Konzultácie týkajúce sa vývoja EPCIP sa uskutočnili so všetkými relevantnými zainteresovanými stranami, a to prostredníctvom:

- prijatia Zelenej knihy o EPCIP 17. novembra 2005, pričom obdobie konzultácií trvalo do 15. januára 2006. Oficiálne odpovede v rámci konzultácií poskytlo 22 členských štátov. K zelenej knihe sa taktiež vyjadrilo asi 100 predstaviteľov súkromného sektora. Odpovede vo všeobecnosti podporovali myšlienku vytvorenia EPCIP,

- Komisia usporiadala tri semináre o ochrane kritickej infraštruktúry (jún 2005, september 2005 a marec 2006). Na všetkých troch seminároch sa zúčastnili zástupcovia členských štátov. Zástupcovia súkromného sektora boli pozvaní na semináre, ktoré sa uskutočnili v septembri 2005 a marci 2006.

- neformálnych stretnutí kontaktných miest CIP. Komisia usporiadala pre kontaktné miesta CIP členských štátov dve stretnutia (v decembri 2005 a vo februári 2006),

- neformálnych stretnutí s predstaviteľmi súkromného sektora. Početné neformálne stretnutia sa uskutočnili so zástupcami niektorých súkromných podnikov, ako aj s priemyselnými združeniami,

- na internej úrovni Komisie pokračovala práca na vývoji EPCIP v rámci pravidelných stretnutí podskupiny pre ochranu kritickej infraštruktúry patriacej do medziútvarovej skupiny pre interné aspekty terorizmu.

5.2. Plánovaná akcia a mechanizmy rozpočtovej intervencie

Odhadovaný vplyv na rozpočet je v priloženom finančnom výkaze.

5.3. Spôsoby implementácie

Keďže ide o smernicu, nie je potrebný žiadny spôsob implementácie rozpočtu.

6. FINANČNÝ VPLYV

6.1. Celkový finančný vplyv na časť B – (počas celého plánovacieho obdobia)

6.1.1. Finančná intervencia

neuv.

6.1.2. Technická a administratívna pomoc, podporné výdavky a výdavky na IT (viazané rozpočtové prostriedky)

neuv.

6.2. Výpočet nákladov na jednotlivé opatrenia plánované v časti B (v rámci celého plánovacieho obdobia)

neuv.

7. VPLYV NA ZAMESTNANCOV A ADMINISTRATÍVNE VÝDAVKY

7.1. Vplyv na ľudské zdroje

Druhy pracovných miest		Zamestnanci poverení riadením akcie za využitia existujúcich zdrojov		Spolu	Opis úloh vyplývajúcich z akcie
		Počet miest na dobu neurčitú	Počet miest na dobu určitú		
Stáli zamestnanci/úradníci alebo dočasní pracovníci	A B C	8 A 1 B	1 C	10	Zhromažďovanie a spracúvanie informácií, príprava zasadnutí výboru
Iné ľudské zdroje					
Celkove		9	1	10	

Potreby týkajúce sa ľudských a administratívnych zdrojov sa pokryjú z prostriedkov pridelených riadiacemu generálnemu riaditeľstvu v rámci ročného procesu prideľovania.

7.2. Celkový finančný vplyv ľudských zdrojov

Druh ľudských zdrojov	Suma (EUR)	Spôsob výpočtu *
Stáli zamestnanci Dočasní pracovníci	1 080 000 48.000	108 000 x 10 = 1 080 000 4 000 x 12 = 48 000
Iné ľudské zdroje (upresnite rozpočtovú položku)		
Celkove	1 128 000	

Sumy predstavujú celkové výdavky za dvanásť mesiacov.

7.3. Ostatné administratívne výdavky vyplývajúce z akcie

Rozpočtová položka (číslo a názov)	Suma (EUR)	Spôsob výpočtu
Celková výška pridelených finančných prostriedkov (hlava A7) A0701 – Služobné cesty A07030 – Zasadnutia A07031 – Povinné výbory A07032 – Nepovinné výbory A07040 – Konferencie A0705 – Štúdie a konzultácie Iné výdavky (uveďte)	24 000 - 128 000 - - - 	2 000 x 12 mesiacov = 24 000 - 32 000 x 4 zasadnutia ročne = 128 000 - - -
Informačné systémy (A-5001/A-4300)	-	-
Iné výdavky - časť A (upresnite)		
Celkove	152 000	

Sumy predstavujú celkové výdavky za dvanásť mesiacov.

Uveďte druh výboru a skupinu, ku ktorej patrí.

I.	Celková suma za rok (7.2 + 7.3)	1 280 000
II.	Trvanie akcie	Priebežne
III.	Celkové náklady na akciu (I x II)	

8. MONITOROVANIE A HODNOTENIE

8.1. Následné opatrenia

neuv.

8.2. Spôsoby a harmonogram plánovaného hodnotenia

neuv.

9. OPATRENIA PROTI PODVODOM

neuv.