KOMISIA EURÓPSKYCH SPOLOČENSTIEV

Brusel, 17.11.2005
KOM(2005) 576 v konečnom znení

# ZELENÁ KNIHA

# O EURÓPSKOM PROGRAME NA OCHRANU NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY

(predložený Komisiou)

# ZELENÁ KNIHA

# O EURÓPSKOM PROGRAME NA OCHRANU NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY

## 1. SÚVISLOSTI

Poškodenie, zničenie alebo porušenie najdôležitejšej infraštruktúry (CI) môže byť spôsobené úmyselnými teroristickými činmi, prírodnými katastrofami, nedbalosťou, nehodami alebo počítačovým pirátstvom, kriminálnou činnosťou a konaním so zlým úmyslom. Na ochranu životov a majetku obyvateľstva EÚ pred rizikom terorizmu, prírodných katastrôf a nehôd, by akékoľvek porušenia alebo manipulácie s najdôležitejšou infraštruktúrou mali byť podľa možnosti krátke, zriedkavé, zvládnuteľné, geograficky izolované a predstavujúce najmenšiu možnú hrozbu pre blahobyt členských štátov, ich občanov a Európskej únie. Nedávne teroristické útoky v Madride a Londýne riziko teroristických útokov proti európskej infraštruktúre zdôraznili. Reakcia EÚ musí byť rýchla, koordinovaná a účinná.

Európska rada na svojom zasadnutí v júni 2004 požiadala Komisiu, aby vypracovala celkovú stratégiu ochrany najdôležitejšej infraštruktúry. V nadväznosti na to Komisia dňa 20. októbra 2004 prijala Oznámenie o ochrane najdôležitejšej infraštruktúry v boji proti terorizmu, v ktorom predložila jasné návrhy možných opatrení na zvýšenie úrovne európskej prevencie, pripravenosti a reakcie na teroristické útoky proti najdôležitejšej infraštruktúre.

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 najdôležitejšej infraštruktúry (EPCIP) a vytvoriť Varovnú informačnú sieť najdôležitejšej infraštruktúry (CIWIN).

Komisia usporiadala dva semináre a vyzvala členské štáty, aby predložili svoje návrhy a pripomienky. Prvý seminár o ochrane najdôležitejšej infraštruktúry EÚ, na ktorom sa zúčastnili členské štáty, sa uskutočnil v dňoch 6. – 7. júna 2005. Po tomto seminári členské štáty poskytli Komisii príslušné podkladové materiály o ich prístupe k ochrane najdôležitejšej infraštruktúry a pripomienky k návrhom, o ktorých sa na seminári diskutovalo. Podklady boli prijaté v júni a júli a stali sa základom ďalšieho rozvoja ochrany najdôležitejšej infraštruktúry. Aby sa diskusia o otázkach ochrany najdôležitejšej infraštruktúry urýchlila, uskutočnil sa druhý seminár o ochrane najdôležitejšej infraštruktúry EÚ, ktorý sa konal v dňoch 12. – 13. septembra. Na seminári sa zúčastnili členské štáty, ako aj priemyselné združenia. Komisia sa nakoniec rozhodla predložiť túto Zelenú knihu, v ktorej načrtáva možnosti pre EPCIP.

## 2. CIEĽ ZELENEJ KNIHY

Hlavným cieľom Zelenej knihy je získať spätnú väzbu v otázke politických alternatív EPCIP zapojením širokého počtu zainteresovaných subjektov. Účinná ochrana najdôležitejšej infraštruktúry si vyžaduje komunikáciu, koordináciu a spoluprácu na vnútroštátnej úrovni a na úrovni EÚ medzi všetkými zainteresovanými subjektami: majiteľmi a prevádzkovateľmi infraštruktúry, regulátormi, profesnými orgánmi a priemyselnými združeniami v spolupráci so všetkými úrovňami vlády a s verejnosťou.

Obsahom Zelenej knihy sú alternatívne spôsoby, ktorými by Komisia mohla reagovať na požiadavku Rady na zavedenie EPCIP a CIWIN a predstavuje druhú fázu konzultačného procesu o zavedení Európskeho programu na ochranu najdôležitejšej infraštruktúry. Komisia očakáva, že predložením tejto Zelenej knihy získa konkrétnu spätnú väzbu k politickým alternatívam, ktoré sú v tomto dokumente načrtnuté. V závislosti od výsledku konzultačného procesu by balík opatrení EPCIP mohol byť predložený v priebehu roku 2006.

## 3. ÚČEL A ROZSAH EPCIP

### 3.1. Globálny cieľ EPCIP

Cieľom EPCIP by bolo zabezpečiť adekvátne a rovnaké úrovne ochranného zabezpečenia najdôležitejšej infraštruktúry, minimálne množstvo slabých miest a rýchle a overené mechanizmy obnovy v rámci celej Únie. Úroveň ochrany možno nebude rovnaká pre všetky typy najdôležitejšej infraštruktúry a môže závisieť od dôsledkov, aké zlyhanie najdôležitejšej infraštruktúry spôsobí. EPCIP by bol nepretržitým procesom a bude potrebná jeho pravidelná revízia, aby sa držal krok s novými problémami a požiadavkami.

EPCIP by mal v najväčšej možnej miere minimalizovať všetky prípadné negatívne dôsledky zvýšených investícií do bezpečnosti na konkurencieschopnosť určitého priemyslu. Pri výpočte proporcionality nákladov je potrebné prihliadať na potrebu zachovania stability trhov, ktorá je pre dlhodobé investície nevyhnutná a na vplyv bezpečnosti na vývoj akciových trhov a napokon na makroekonomický rozmer.

**Otázka**

Je to vhodný cieľ EPCIP? Ak nie, aký by mal byť?

### 3.2. Pred čím by mal EPCIP chrániť

Hoci opatrenia týkajúce sa riadenia následkov sú pre väčšinu narušení zhodné, resp. podobné, ochranné opatrenia sa môžu líšiť v závislosti od povahy hrozby. Medzi hrozby, ktoré by podstatne znížili schopnosť zabezpečovať základné potreby a bezpečnosť obyvateľstva, udržať poriadok a poskytovať minimálne základné verejné služby alebo riadne fungovanie ekonomiky, patria úmyselné útoky a prírodné katastrofy. Možnosti sú:

a) **úplná ochrana pred nebezpečenstvami každého druhu** – Išlo by o komplexný prístup zohľadňujúci hrozbu vyplývajúcu tak z úmyselných útokov ako aj prírodných katastrôf. Tento prístup by zabezpečil úplné využitie súčinností medzi ochrannými opatreniami, nekládol by však nejaký väčší dôraz na terorizmus;

b) **ochrana pred nebezpečenstvami každého druhu so zameraním na terorizmus** – Išlo by o flexibilný prístup zabezpečujúci prepojenie s ostatnými druhmi nebezpečenstiev (hrozba vyplývajúca z úmyselných útokov ako aj prírodných katastrôf), prioritou by však bol terorizmus. Ak bude úroveň ochranných opatrení v určitom priemyselnom odvetví primeraná, zainteresované subjekty sa môžu sústrediť na tie hrozby, voči ktorým sú stále zraniteľné.

c) **ochrana pred nebezpečenstvom terorizmu** – Išlo by o prístup zameraný na terorizmus, bez osobitnejšieho dôrazu na všeobecnejšie hrozby.

**Otázka**

Aký prístup by sa mal pre EPCIP zvoliť? Prečo?

## 4. NAVRHOVANÉ KĽÚČOVÉ ZÁSADY

EPCIP by sa mal zakladať na týchto navrhovaných kľúčových zásadách:

- **Subsidiarita** – Základ EPCIP by tvorila subsidiarita, teda ochrana najdôležitejšej infraštruktúry by bola predovšetkým zodpovednosťou na vnútroštátnej úrovni. Hlavnú zodpovednosť za ochranu najdôležitejšej infraštruktúry by niesli členské štáty a majitelia/prevádzkovatelia pôsobiaci na základe spoločného rámca. Komisia by sa zase sústredila na aspekty týkajúce sa ochrany najdôležitejšej infraštruktúry cezhraničného charakteru. Povinnosť a zodpovednosť majiteľov a prevádzkovateľov za prijatie vlastných rozhodnutí a plánov na ochranu svojich vlastných majetkových hodnôt by zostala bezo zmeny.

- **Komplementarita** – Spoločný rámec EPCIP by bol doplnkom k existujúcim opatreniam. Zavedené mechanizmy Spoločenstva by sa mali naďalej používať a mali by pomôcť zaistiť celkovú implementáciu EPCIP.

- **Dôvernosť** – Zdieľanie informácií súvisiacich s ochranou najdôležitejšej infraštruktúry by sa uskutočňovalo v dôvernom prostredí. To je nevyhnutné, ak si uvedomíme, že využitie informácií o majetkových hodnotách najdôležitejšej infraštruktúry môže spôsobiť zlyhanie alebo neprijateľné následky pre zariadenia najdôležitejšej infraštruktúry. Na úrovni EÚ a členských štátov by informácie súvisiace s ochranou najdôležitejšej infraštruktúry boli klasifikované a prístup k nim by sa udelil len na základe existencie „potreby byť informovaný“.

- **Spolupráca zainteresovaných subjektov** – Pri ochrane najdôležitejšej infraštruktúry zohrávajú svoju úlohu všetky zainteresované strany vrátane členských štátov, Komisie, priemyselných/obchodných združení, normalizačných orgánov a majiteľov, prevádzkovateľov a užívateľov („užívatelia“ sú definovaní ako organizácie, ktoré využívajú a používajú infraštruktúru na účely obchodu a poskytovania služieb). Všetky zainteresované subjekty by mali spolupracovať a prispievať k vypracovaniu a implementácii EPCIP v súlade s ich špecifickými úlohami a zodpovednosťami. Orgány členských štátov by zabezpečovali vedenie a koordináciu pri vypracovávaní a implementácii národného jednotného prístupu k ochrane najdôležitejšej infraštruktúry v rámci svojich jurisdikcií. Majitelia, prevádzkovatelia a užívatelia by boli aktívne zapojení tak na vnútroštátnej úrovni, ako aj na úrovni EÚ. Ak neexistujú sektorové normy, alebo ak ešte neboli zavedené medzinárodné predpisy, normalizačné orgány by v prípade potreby mohli prijať jednotné normy.

- **Proporcionalita** – Stratégie a opatrenia týkajúce sa ochrany by boli primerané k úrovni príslušného rizika, nakoľko nie všetky typy infraštruktúry možno chrániť pred všetkými hrozbami (napríklad, elektrické prenosové siete sú príliš veľké, aby mohli byť ohradené alebo strážené). Uplatňovaním vhodných postupov riadenia rizika sa môže pozornosť sústrediť na najrizikovejšie oblasti, zohľadňujúc hrozbu, relatívnu dôležitosť, pomer nákladov a prínosov, úroveň ochranného zabezpečenia a efektívnosť dostupných stratégií pre zmierňovanie rizika.

**Otázka**

Sú tieto kľúčové zásady prijateľné? Nie sú niektoré z nich nadbytočné? Existujú nejaké ďalšie, ktoré by mali byť zvážené?

Súhlasíte s tým, že ochranné opatrenia by mali byť primerané k úrovni príslušného rizika, nakoľko nie všetku infraštruktúru možno chrániť pred všetkými hrozbami?

## 5. SPOLOČNÝ RÁMEC EPCIP

Poškodenie alebo zničenie časti infraštruktúry v jednom členskom štáte môže mať nepriaznivý vplyv na niekoľkých 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 mnoho typov 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.

Účinná ochrana si vyžaduje komunikáciu, koordináciu a spoluprácu na vnútroštátnej úrovni, na úrovni EÚ (v prípade potreby) a na medzinárodnej úrovni medzi všetkými zainteresovanými subjektami. Mohol by byť zavedený spoločný rámec EÚ na ochranu najdôležitejšej infraštruktúry v Európe, aby sa zabezpečilo, že každý členský štát poskytuje primeranú a rovnakú úroveň ochrany v súvislosti s jeho najdôležitejšou infraštruktúrou a že sa neporušujú pravidlá hospodárskej súťaže v rámci vnútorného trhu. S cieľom podporiť činnosti členských štátov by Komisia poskytnutím spoločného rámca pre ochranu najdôležitejšej infraštruktúry uľahčila určenie, výmenu a rozširovanie osvedčených postupov vo vzťahu k otázkam súvisiacim s ochranou najdôležitejšej infraštruktúry. Rozsah tohto všeobecného rámca je potrebné zvážiť.

Spoločný rámec EPCIP by obsahoval horizontálne opatrenia, ktoré by definovali kompetencie a zodpovednosti všetkých zainteresovaných subjektov vo vzťahu k ochrane najdôležitejšej infraštruktúry (CIP) a zároveň vytvárali základ pre prístupy podľa jednotlivých sektorov. Spoločný rámec by mal dopĺňať existujúce sektorové opatrenia na úrovni Spoločenstva a členských štátov s cieľom zabezpečiť najvyššiu možnú úroveň ochrany najdôležitejšej infraštruktúry v Európskej únii. Prioritou by malo byť dosiahnutie dohody o spoločnom zozname definícií a sektorov najdôležitejšej infraštruktúry.

Nakoľko jednotlivé sektory, pod ktoré najdôležitejšia infraštruktúra spadá, sa značne líšia, bolo by ťažké v horizontálnom rámci presne stanoviť kritériá, ktoré by sa mali použiť pri určovaní a ochrane všetkých z nich. Tieto by sa mali vypracovať osobitne pre každý jednotlivý sektor. Napriek tomu je však potrebné spoločné chápanie určitých prierezových otázok.

Preto sa navrhuje, aby sa posilnenie najdôležitejšej infraštruktúry v EÚ dosiahlo stanovením spoločného rámca EPCIP (spoločné ciele, metodika napr. pre porovnávanie, vzájomné závislosti) na základe výmeny osvedčených postupov a mechanizmov monitorovania plnenia. Medzi prvky, ktoré by tvorili časť spoločného rámca, patria:

- spoločné zásady ochrany najdôležitejšej infraštruktúry,
- spoločne dohodnuté kódy/normy,

- spoločné definície, na základe ktorých možno dohodnúť špecifické definície pre jednotlivé sektory (indikatívny zoznam definícií tvorí prílohu 1),
- spoločný zoznam sektorov najdôležitejšej infraštruktúry (indikatívny zoznam sektorov tvorí prílohu 2),
- prioritné oblasti ochrany najdôležitejšej infraštruktúry,
- opis zodpovedností príslušných zainteresovaných subjektov,
- dohodnuté referenčné kritériá,
- metodika pre porovnanie infraštruktúry v rôznych sektoroch a stanovenie priorít.

Takýto spoločný rámec by tiež minimalizoval prípadné vnútorný trh narúšajúce účinky.

Spoločný rámec programu EPCIP by mohol byť dobrovoľný alebo povinný, resp. zmiešaný v závislosti od toho, o akú otázku sa jedná. Oba typy rámca by mohli dopĺňať existujúce sektorové a horizontálne opatrenia na úrovni Spoločenstva a na úrovni členských štátov, avšak len právny rámec by poskytoval silný a vymožiteľný právny základ pre súdržnú a jednotnú implementáciu opatrení na ochranu najdôležitejšej infraštruktúry EÚ, ako aj jasné definovanie príslušných zodpovedností členských štátov a Komisie. Nezáväzné dobrovoľné opatrenia sú síce pružné, ale neposkytovali by jasné stanovenie povinností jednotlivých subjektov.

V závislosti od výsledku dôkladnej analýzy a venovaním náležitej pozornosti proporcionalite navrhovaných opatrení môže Komisia pri svojom návrhu EPCIP využiť množstvo nástrojov vrátane legislatívy. Návrhy špecifických opatrení budú v prípade potreby doplnené hodnotením dopadu.

**Otázky**

Bol by spoločný rámec pri posilňovaní ochrany najdôležitejšej infraštruktúry účinný?

Ak by sa vyžadoval legislatívny rámec, aké prvky by mal obsahovať?

Súhlasíte s tým, že kritériá pre definovanie jednotlivých druhov najdôležitejšej infraštruktúry EÚ a príslušné ochranné opatrenia by mali byť určené podľa jednotlivých sektorov?

Pomohol by spoločný rámec vyjasniť zodpovednosti príslušných zainteresovaných subjektov? Do akej miery by mal byť takýto spoločný rámec povinný a do akej miery dobrovoľný?

Aký by mal byť rozsah spoločného rámca? Súhlasíte s indikatívnym zoznamom pojmov a definícií v prílohe I, na základe ktorých sa môžu vypracovať špecifické definície (v prípade potreby)? Súhlasíte s indikatívnym zoznamom sektorov najdôležitejšej infraštruktúry v prílohe II?

## 6. NAJDÔLEŽITEJŠIA INFRAŠTRUKTÚRA EÚ (ECI)

### 6.1. Definícia najdôležitejšej infraštruktúry EÚ

Definícia predmetu najdôležitejšej infraštruktúry EÚ by bola stanovená jej cezhraničným účinkom, ktorý určuje, či by incident mohol mať vážny dopad mimo územia členského štátu, v ktorom sa zariadenie nachádza. Ďalším prvkom, ktorý by sa mal zohľadniť, je skutočnosť, že schémy dvojstrannej spolupráce pri ochrane najdôležitejšej infraštruktúry medzi členskými štátmi predstavujú dobre zavedené a účinné prostriedky zaobchádzania s najdôležitejšou

infraštruktúrou medzi hranicami dvoch členských štátov. Takáto spolupráca by bola doplnková k EPCIP.

Najdôležitejšia infraštruktúra EÚ by mohla pozostávať z tých fyzických zdrojov, služieb, informačno-technologických zariadení, sietí a majetkových hodnôt infraštruktúry, ktorých porušenie alebo zničenie by malo vážny dopad na zdravie, bezpečnosť, istotu a ekonomický alebo sociálny blahobyt buď:

a) dvoch alebo viacerých členských štátov – **to by zahŕňalo určitú najdôležitejšiu infraštruktúru na dvojstrannej úrovni (v prípade potreby);** alebo

b) troch alebo viacerých členských štátov – **to by vylučovalo všetku najdôležitejšiu infraštruktúru na dvojstrannej úrovni.**

Pri zvažovaní príslušných výhod týchto možností je dôležité prihliadať na tieto skutočnosti:

– skutočnosť, že časť infraštruktúry by bola označená za najdôležitejšiu infraštruktúru EÚ neznamená, že by si nevyhnutne vyžadovala akékoľvek dodatočné ochranné opatrenia. Existujúce ochranné opatrenia, ktoré by mohli zahŕňať dvojstranné dohody medzi členskými štátmi, môžu byť úplne primerané a ich označením za najdôležitejšiu infraštruktúru EÚ sa nezmenia,

– s možnosťou a) môže byť spojené väčšie množstvo označení,

– možnosť b) môže znamenať, že pri infraštruktúre, ktorá sa týka len dvoch členských štátov, by Spoločenstvo nezohrávalo žiadnu úlohu, aj keby jeden z týchto dvoch členských štátov považoval úroveň ochrany za nedostatočnú a ostatné členské štáty by odmietli podniknúť akékoľvek kroky. Možnosť b) by tiež mohla viesť k množstvu dvojstranných dohôd alebo nezhôd medzi členskými štátmi. Takisto priemysel, ktorý obvykle funguje na paneurópskej úrovni, by bol možno nútený pracovať s nesúrodou mozaikou rôznych dohôd, čo by mohlo viesť k dodatočným nákladom.

Do úvahy by sa mala zobrať aj najdôležitejšia infraštruktúra s pôvodom alebo pôsobením mimo EÚ, ale s prepojením alebo s potenciálnym priamym účinkom na členské štáty EÚ.

**Otázka**

Mala by byť najdôležitejšia infraštruktúra EÚ infraštruktúrou s potenciálnym vážnym cezhraničným dopadom na dva alebo viac členských štátov, alebo tri alebo viac členských štátov? Prečo?

### 6.2. Vzájomné závislosti

Navrhuje sa, aby postupné určovanie všetkej najdôležitejšej infraštruktúry EÚ bralo do úvahy najmä vzájomné závislosti. Štúdie o vzájomných závislostiach by prispeli k hodnoteniu potenciálneho dopadu hrozieb voči určitej najdôležitejšej infraštruktúre a najmä k stanoveniu, ktoré členské štáty by boli v prípade veľkého incidentu spojeného s najdôležitejšou infraštruktúrou najviac ovplyvnené.

Plne by sa zohľadnili vzájomné závislosti v rámci a medzi podnikateľskými subjektami, priemyselnými sektormi, geografickými jurisdikciami a orgánmi členských štátov, najmä tých, ktoré sú vybavené informačnými a komunikačnými technológiami (IKT). Komisia,

členské štáty a majitelia/prevádzkovatelia najdôležitejšej infraštruktúry by mali spoločne pracovať na určení týchto vzájomných závislostí a uplatniť vhodné stratégie na zníženie možného rizika.

**Otázka**

Ako možno zohľadniť vzájomné závislosti?

Poznáte nejaké vhodné metodiky pre analýzu vzájomných závislostí?

Na akej úrovni by malo prebiehať určovanie vzájomných závislostí – na úrovni EÚ a/alebo na úrovni členských štátov?

### 6.3. Kroky implementácie pre najdôležitejšiu infraštruktúru EÚ

Komisia navrhuje tieto kroky implementácie pre najdôležitejšiu infraštruktúru EÚ:

(1) Komisia v spolupráci s členskými štátmi vypracuje špecifické kritériá, ktoré by sa použili na určenie najdôležitejšej infraštruktúry EÚ podľa jednotlivých sektorov;

(2) Postupné určovanie a overovanie najdôležitejšej infraštruktúry EÚ podľa jednotlivých sektorov zo strany členských štátov a Komisie. Rozhodnutie o označení určitej najdôležitejšej infraštruktúry za najdôležitejšiu infraštruktúru EÚ sa prijme na európskej úrovni[1] z dôvodu cezhraničného charakteru predmetnej infraštruktúry;

(3) Členské štáty a Komisia analyzujú medzery súčasnej bezpečnosti vo vzťahu k najdôležitejšej infraštruktúre EÚ podľa jednotlivých sektorov;

(4) Členské štáty a Komisia sa dohodnú na prioritných sektoroch/infraštruktúre, v ktorých sa má konať, pričom zohľadnia vzájomné závislosti;

(5) V prípade potreby sa Komisia a najdôležitejšie zainteresované subjekty členských štátov dohodnú na návrhoch minimálnych ochranných opatrení, ktoré by mohli zahŕňať normy;

(6) Po prijatí návrhov Radou sa tieto opatrenia následne implementujú;

(7) Pravidelné monitorovanie zabezpečujú členské štáty a Komisia. V prípade potreby sa vykonávajú revízie (opatrení a určenia najdôležitejšej infraštruktúry).

**Otázky**

Je zoznam krokov týkajúcich sa implementácie najdôležitejšej infraštruktúry EÚ prijateľný?

Ako navrhujete, aby Komisia a členské štáty spoločne označili najdôležitejšiu infraštruktúru EÚ – členské štáty majú odborné znalosti, Komisia pozná európske záujmy? Malo by to byť právne rozhodnutie?

[1] S výnimkou infraštruktúry súvisiacej s obranou.

Je potrebný arbitrážny mechanizmus v prípade, že určitý členský štát nesúhlasí s označením infraštruktúry v rámci jeho jurisdikcie za najdôležitejšiu infraštruktúru EÚ?

Je potrebné overovať takéto označenia? Kto by mal byť zodpovedný?

Mali by mať členské štáty možnosť označiť infraštruktúru v iných členských štátoch alebo tretích krajinách za najdôležitejšiu z ich pohľadu? Čo by sa malo stať, ak členský štát, tretia krajina alebo priemysel považuje časť infraštruktúry v členskom štáte za najdôležitejšiu z ich pohľadu?

Čo by sa malo stať, ak ju členský štát neurčí? Je potrebný odvolací mechanizmus? Ak áno, prečo?

Mal by mať prevádzkovateľ možnosť odvolať sa v prípade, ak nesúhlasia s jeho označením, resp. neoznačením? Ak áno, kde?

Aké metodiky je potrebné vypracovať na stanovenie prioritných sektorov/infraštruktúry, v ktorých sa má konať? Existujú už vhodné metodiky, ktoré by mohli byť prispôsobené na európsku úroveň?

Ako sa Komisia môže zapojiť do analýzy bezpečnostných medzier v oblasti ochrany najdôležitejšej infraštruktúry EÚ?

## 7. NAJDÔLEŽITEJŠIA INFRAŠTRUKTÚRA ČLENSKÉHO ŠTÁTU (NCI)

### 7.1. Úloha najdôležitejšej infraštruktúry členského štátu v rámci EPCIP

Mnoho európskych spoločností pôsobí na cezhraničnej úrovni, a preto majú vo vzťahu k najdôležitejšej infraštruktúre členského štátu rozličné povinnosti. Preto sa v záujme členských štátov a EÚ ako celku navrhuje, aby každý členský štát chránil svoju najdôležitejšiu infraštruktúru na základe spoločného rámca tak, aby majitelia a prevádzkovatelia po celej Európe nepodliehali rôznorodej zmesi rámcov, z ktorej by vyplývalo množstvo metodík a dodatočné náklady. V tomto zmysle Komisia navrhuje, aby EPCIP, ktorý sa zameriava predovšetkým na najdôležitejšiu infraštruktúru EÚ, úplne nevynechal najdôležitejšiu infraštruktúru členského štátu. Do úvahy prichádzajú tri možnosti:

**a) najdôležitejšia infraštruktúra členského štátu je plne zahrnutá do EPCIP;**

**b) najdôležitejšia infraštruktúra členského štátu nespadá do rámca EPCIP;**

**c) členské štáty môžu na základe svojho vlastného uváženia použiť vo vzťahu k najdôležitejšej infraštruktúre členského štátu časti EPCIP, nie je to však ich povinnosťou.**

**Otázka**

Účinná ochrana najdôležitejšej infraštruktúry v Európskej únii by si pravdepodobne vyžadovala určenie tak najdôležitejšej infraštruktúry EÚ, ako aj najdôležitejšej infraštruktúry členského štátu. Súhlasíte s tým, že hoci by sa EPCIP mal zamerať na najdôležitejšiu infraštruktúru EÚ, najdôležitejšiu infraštruktúru členského štátu nemožno úplne vynechať?

Ktorá z týchto možností je podľa Vás pre EPCIP najvhodnejšia?

### 7.2. Národné programy na ochranu najdôležitejšej infraštruktúry

Na základe spoločného rámca EPCIP by členské štáty mohli pre najdôležitejšiu infraštruktúru členského štátu vypracovať národné programy na ochranu najdôležitejšej infraštruktúry. Členské štáty by mohli uplatniť prísnejšie opatrenia než tie, ktoré sa uplatňujú v rámci EPCIP.

**Otázka**

Je žiadúce, aby každý členský štát na základe EPCIP prijal svoj národný program na ochranu najdôležitejšej infraštruktúry?

### 7.3. Jediný orgán dohľadu

Vzhľadom na potrebu účinnosti a súdržnosti je nevyhnutné, aby každý členský štát určil jediný orgán dohľadu, ktorý by sa zaoberal celkovou implementáciou EPCIP. Do úvahy prichádzajú dve možnosti:

a) jediný orgán dohľadu nad ochranou najdôležitejšej infraštruktúry;

b) národný kontaktný orgán bez právomoci, s ponechaním rozhodnutia o zabezpečení v tejto oblasti na členských štátoch.

Takýto orgán by mohol koordinovať, monitorovať a dohliadať na implementáciu EPCIP v rámci svojej jurisdikcie a mohol by pôsobiť ako hlavný inštitucionálny kontaktný orgán pre otázky ochrany najdôležitejšej infraštruktúry vo vzťahu ku Komisii, ostatným členským štátom a majiteľom a prevádzkovateľom najdôležitejšej infraštruktúry. Tento orgán by mohol tvoriť základ pre národné zastúpenie v expertných skupinách zaoberajúcich sa otázkami ochrany najdôležitejšej infraštruktúry a mohol by byť napojený na Varovnú informačnú sieť najdôležitejšej infraštruktúry (CIWIN). Národný koordinačný orgán pre ochranu najdôležitejšej infraštruktúry (NCCB) by mohol koordinovať otázky ochrany najdôležitejšej infraštruktúry členského štátu bez ohľadu na skutočnosť, že do problematiky ochrany najdôležitejšej infraštruktúry už môžu byť zapojené iné orgány alebo subjekty.

Postupné určovanie najdôležitejšej infraštruktúry členského štátu možno dosiahnuť tak, že sa majiteľom a prevádzkovateľom infraštruktúry stanoví povinnosť informovať Národný koordinačný orgán pre ochranu najdôležitejšej infraštruktúry o všetkých obchodných činnostiach, ktoré súvisia s ochranou najdôležitejšej infraštruktúry.

Národný koordinačný orgán pre ochranu najdôležitejšej infraštruktúry by mohol byť zodpovedný za právne záväzné rozhodnutie o označení infraštruktúry v rámci svojej jurisdikcie za najdôležitejšiu infraštruktúru členského štátu. Touto informáciou by disponoval výhradne iba príslušný členský štát.

Konkrétne kompetencie by mohli zahŕňať:

a) koordináciu, monitorovanie a dohľad nad celkovou implementáciou EPCIP v členskom štáte;

b) pôsobenie ako hlavný inštitucionálny kontaktný orgán pre otázky ochrany najdôležitejšej infraštruktúry vo vzťahu ku:

   i. Komisii;

   ii. ostatným členským štátom;

   iii. majiteľom a prevádzkovateľom najdôležitejšej infraštruktúry;

c) účasť na označovaní najdôležitejšej infraštruktúry EÚ;

d) prijatie právne záväzného rozhodnutia o označení infraštruktúry v rámci svojej jurisdikcie za najdôležitejšiu infraštruktúru členského štátu;

e) pôsobenie ako odvolací orgán pre majiteľov/prevádzkovateľov, ktorí nesúhlasia s označením ich infraštruktúry za „najdôležitejšiu infraštruktúru“;

f) účasť na vypracovaní národného programu na ochranu najdôležitejšej infraštruktúry a sektorových programov na ochranu najdôležitejšej infraštruktúry;

g) určenie vzájomných závislostí medzi jednotlivými sektormi najdôležitejšej infraštruktúry;

h) prispievanie k sektorovým prístupom k ochrane najdôležitejšej infraštruktúry prostredníctvom účasti v expertných skupinách. Do expertných skupín by mohli byť prizývaní zástupcovia majiteľov a prevádzkovateľov, aby sa zúčastňovali a prispievali do diskusie. Stretnutia by sa mohli konať na pravidelnom základe;

i) dohľad nad procesom prípravy s najdôležitejšou infraštruktúrou súvisiacich pohotovostných plánov.

**Otázky**

Súhlasíte s tým, že členské štáty by mali byť samé zodpovedné za označenie a riadenie najdôležitejšej infraštruktúry členského štátu na základe spoločného rámca EPCIP?

Je potrebné, aby bol v každom členskom štáte určený koordinačný orgán pre ochranu najdôležitejšej infraštruktúry, ktorý by bol zodpovedný za celkovú koordináciu opatrení súvisiacich s ochranou najdôležitejšej infraštruktúry, pri súčasnom zachovaní existujúcich zodpovedností v rámci jednotlivých sektorov (orgány civilného letectva, smernica Seveso, atď.)?

Boli by navrhované kompetencie takéhoto koordinačného orgánu primerané? Sú potrebné nejaké ďalšie?

### 7.4. Kroky implementácie pre najdôležitejšiu infraštruktúru členského štátu

Komisia navrhuje tieto kroky implementácie pre najdôležitejšiu infraštruktúru členského štátu:

(1) Členské štáty na základe EPCIP vypracujú špecifické kritériá, ktoré by sa použili na určenie najdôležitejšej infraštruktúry členského štátu;

(2) Členské štáty postupne určujú a overujú najdôležitejšiu infraštruktúru členského štátu podľa jednotlivých sektorov;

(3) Členské štáty analyzujú existujúce bezpečnostné medzery vo vzťahu k najdôležitejšej infraštruktúre členského štátu podľa jednotlivých sektorov;

(4) Členské štáty stanovia prioritné sektory, v ktorých sa má konať, pričom zohľadnia vzájomné závislosti a príslušné priority dohodnuté na úrovni EÚ;

(5) V prípade potreby členské štáty pre každý sektor dohodnú minimálne ochranné opatrenia;

(6) Členské štáty sú povinné zabezpečiť, aby majitelia/prevádzkovatelia v rámci ich jurisdikcie vykonávali potrebné implementačné opatrenia;

(7) Členské štáty zabezpečujú pravidelné monitorovanie. V prípade potreby sa vykonávajú revízie (opatrení a určenia najdôležitejšej infraštruktúry).

**Otázka**

Je zoznam krokov týkajúcich sa implementácie najdôležitejšej infraštruktúry členského štátu prijateľný? Nie sú niektoré kroky nadbytočné? Mali by byť nejaké kroky doplnené?

## 8. ÚLOHA MAJITEĽOV, PREVÁDZKOVATEĽOV A UŽÍVATEĽOV NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY

### 8.1. Zodpovednosti majiteľov, prevádzkovateľov a užívateľov najdôležitejšej infraštruktúry

Označenie za najdôležitejšiu infraštruktúru prináša majiteľom a prevádzkovateľom určité zodpovednosti. Do úvahy prichádzajú štyri zodpovednosti pre majiteľov a prevádzkovateľov v súvislosti s označením za najdôležitejšiu infraštruktúru členského štátu alebo najdôležitejšiu infraštruktúru EÚ:

**(1) Oznámenie skutočnosti, že infraštruktúra by sa mohla považovať za najdôležitejšiu, a to príslušnému orgánu ochrany najdôležitejšej infraštruktúry členského štátu;**

**(2) Určenie vysokopostaveného(-ých) zástupcu(-ov), ktorý(-í) bude(-ú) pôsobiť ako styčný úradník pre bezpečnosť (SLO) medzi majiteľom/prevádzkovateľom a príslušným orgánom ochrany najdôležitejšej infraštruktúry členského štátu.** Styčný úradník pre bezpečnosť by sa podieľal na vypracovávaní bezpečnostných a pohotovostných

plánov. Bol by hlavným úradníkom pre styk s orgánom ochrany najdôležitejšej infraštruktúry príslušného sektora v členskom štáte a prípadne s orgánmi presadzovania práva;

**(3) Vypracovanie, implementácia a aktualizácia bezpečnostného plánu (OSP).** Navrhovaná štruktúra bezpečnostného plánu tvorí prílohu 3;

**(4) Účasť na vypracovaní pohotovostného plánu** pre najdôležitejšiu infraštruktúru v spolupráci s civilnou ochranou príslušného členského štátu a prípadne s orgánmi presadzovania práva.

Bezpečnostný plán by sa mohol predložiť na schválenie orgánu ochrany najdôležitejšej infraštruktúry daného sektora príslušného členského štátu v rámci celkového dohľadu Národného koordinačného orgánu pre ochranu najdôležitejšej infraštruktúry bez ohľadu na to, či ide o najdôležitejšiu infraštruktúru členského štátu alebo najdôležitejšiu infraštruktúru EÚ, ktorý by zabezpečil jednotnosť bezpečnostných opatrení prijatých jednotlivými majiteľmi a prevádzkovateľmi a v príslušných sektoroch vo všeobecnosti. Majitelia a prevádzkovatelia by zase prostredníctvom Národného koordinačného orgánu pre ochranu najdôležitejšej infraštruktúry, prípadne prostredníctvom Komisie mohli získať primeranú spätnú väzbu a podporu v oblasti príslušných hrozieb, rozvoja osvedčených postupov a prípadne pomoc pri stanovovaní vzájomných závislostí a zraniteľných miest.

Každý členský štát by mohol stanoviť časové limity na vypracovanie bezpečnostného plánu zo strany majiteľov a prevádzkovateľov najdôležitejšej infraštruktúry členského štátu a najdôležitejšej infraštruktúry EÚ (v prípade najdôležitejšej infraštruktúry EÚ by bola zapojená aj Komisia) a mohol by stanoviť administratívne pokuty v prípade, že sa tieto termíny nedodržia.

Navrhuje sa, že bezpečnostný plán by mal určiť majetkové hodnoty najdôležitejšej infraštruktúry majiteľa/prevádzkovateľa a obsahovať príslušné bezpečnostné riešenia na ich ochranu. Mal by opisovať metódy a postupy, ktoré je potrebné dodržať, aby sa zabezpečil súlad s programom EPCIP, národnými programami na ochranu najdôležitejšej infraštruktúry a príslušnými sektorovými programami na ochranu najdôležitejšej infraštruktúry. Bezpečnostný plán predstavuje v rámci regulácie ochrany najdôležitejšej infraštruktúry prostriedok prístupu „zdola hore“, ktorý poskytuje väčšiu voľnosť (a tiež väčšiu zodpovednosť) súkromnému sektoru.

Najmä v prípadoch určitého typu infraštruktúry, ako napr. elektrické rozvodné siete a informačné siete, by bolo nereálne (z praktického a finančného hľadiska) predpokladať, že majitelia a prevádzkovatelia zabezpečia rovnakú úroveň ochrany vo vzťahu ku všetkým svojim majetkovým hodnotám. V takýchto prípadoch sa navrhuje, aby majitelia a prevádzkovatelia mali možnosť v spolupráci s príslušnými orgánmi určiť najdôležitejšie body (uzly) fyzickej alebo informačnej siete, na ktoré by sa mohli ochranné bezpečnostné opatrenia zamerať.

Bezpečnostný plán by mohol obsahovať dve skupiny bezpečnostných opatrení:

- **stále bezpečnostné opatrenia**, ktoré by určovali nevyhnutné bezpečnostné investície a prostriedky, ktoré majiteľ/prevádzkovateľ nedokáže nainštalovať alebo mobilizovať v krátkom čase. Majiteľ/prevádzkovateľ by vo vzťahu

k potenciálnym hrozbám zabezpečoval stav trvalej pohotovosti, ktorý by nenarušil jeho bežné ekonomické, administratívne a sociálne činnosti,

- **odstupňované bezpečnostné opatrenia**, ktoré by sa mohli uplatniť v závislosti od rôznych úrovní hrozieb. Bezpečnostný plán by tak predpokladal rôzne režimy bezpečnosti, ktoré by sa menili podľa prípadných úrovní hrozieb v členských štátoch, kde je infraštruktúra situovaná.

Navrhuje sa, aby v prípade, že si majiteľ/prevádzkovateľ najdôležitejšej infraštruktúry nesplní povinnosť vypracovať bezpečnostný plán, zúčastniť sa na vypracovaní pohotovostných plánov a určiť styčného úradníka pre bezpečnosť, bola vytvorená možnosť uložiť peňažnú pokutu.

**Otázky**

Sú potenciálne zodpovednosti majiteľov/prevádzkovateľov najdôležitejšej infraštruktúry prijateľné v zmysle zvyšovania bezpečnosti najdôležitejšej infraštruktúry? Aké by boli ich predpokladané náklady?

Mali by byť majitelia a prevádzkovatelia povinní oznámiť, že ich infraštruktúra môže mať charakter najdôležitejšej infraštruktúry? Myslíte si, že vypracovanie bezpečnostného plánu je potrebné? Prečo?

Sú navrhované povinnosti primerané vzhľadom na s nimi spojené náklady?

Aké práva by orgány členských štátov a Komisia mohli udeliť majiteľom a prevádzkovateľom najdôležitejšej infraštruktúry?

### 8.2. Dialóg s majiteľmi, prevádzkovateľmi a užívateľmi najdôležitejšej infraštruktúry

EPCIP by mohol zapojiť majiteľov a prevádzkovateľov do partnerstiev. Úspech akýchkoľvek programov ochrany závisí od spolupráce a úrovne zaangažovanosti zo strany majiteľov a prevádzkovateľov. Majitelia a prevádzkovatelia najdôležitejšej infraštruktúry by v rámci členských štátov mohli byť zapojení do rozvoja ochrany najdôležitejšej infraštruktúry prostredníctvom pravidelných kontaktov s Národným koordinačným orgánom pre ochranu najdôležitejšej infraštruktúry.

Na úrovni EÚ by mohli vzniknúť fóra s cieľom uľahčiť výmenu názorov na otázky všeobecnej a sektorovej ochrany najdôležitejšej infraštruktúry. Spoločný prístup k zapojeniu súkromného sektora do problematiky ochrany najdôležitejšej infraštruktúry s cieľom spojiť zainteresované subjekty verejného a súkromného sektora by členským štátom, Komisii a priemyslu poskytlo dôležitú platformu pre komunikáciu o akejkoľvek novovzniknutej otázke vo vzťahu k ochrane najdôležitejšej infraštruktúry. Majitelia, prevádzkovatelia a užívatelia najdôležitejšej infraštruktúry by mohli byť zapojení do vypracovania spoločných usmernení, noriem osvedčených postupov a prípadne zdieľania informácií. Takýto dialóg by pomohol usmerniť budúce revízie EPCIP.

V prípade potreby by Komisia mohla podporiť vznik priemyselných/obchodných združení súvisiacich s ochranou najdôležitejšej infraštruktúry v EÚ. Dvomi hlavnými cieľmi by bolo zabezpečenie udržania konkurencieschopnosti európskeho priemyslu a posilnenie bezpečnosti občanov EÚ.

**Otázka**

Aká by mala byť štruktúra dialógu s majiteľmi, prevádzkovateľmi a užívateľmi najdôležitejšej infraštruktúry?

Kto by mal majiteľov, prevádzkovateľov a užívateľov vo verejno-súkromnom dialógu zastupovať?

## 9. PODPORNÉ OPATRENIA VO VZŤAHU K EPCIP

### 9.1. Varovná informačná sieť najdôležitejšej infraštruktúry (CIWIN)

Komisia vyvinula celý rad systémov rýchleho varovania, ktoré umožňujú konkrétne, koordinovane a účinne reagovať v prípade mimoriadnych situácií vrátane prípadov teroristického pôvodu. Dňa 20. októbra 2004 Komisia oznámila vytvorenie centrálnej siete v Komisii, zabezpečujúcej rýchly tok informácií medzi všetkými systémami rýchleho varovania v Komisii a jej príslušných útvaroch (ARGUS).

Komisia navrhuje vytvorenie siete CIWIN, ktorá by mohla podporiť vypracovanie vhodných ochranných opatrení zjednodušením výmeny osvedčených postupov bezpečným spôsobom ako aj tým, že bude slúžiť ako prostriedok prenosu bezprostredných hrozieb a varovaní. Systém by zabezpečoval, aby mali správni ľudia správne informácie v správnom čase.

Pre vytvorenie CIWIN prichádzajú do úvahy tieto tri možnosti:

(1) **CIWIN by mala podobu fóra obmedzeného na výmenu návrhov a osvedčených postupov v súvislosti s ochranou najdôležitejšej infraštruktúry** na podporu majiteľov a prevádzkovateľov najdôležitejšej infraštruktúry. Takéto fórum by mohlo pozostávať zo siete expertov a elektronickej platformy pre výmenu príslušných informácií v bezpečnom prostredí. Komisia by zohrávala významnú úlohu pri zhromažďovaní a rozširovaní takýchto informácií. Táto možnosť by nezahŕňala nevyhnutné rýchle varovania o bezprostredných hrozbách. V budúcnosti by však bol priestor na rozšírenie CIWIN;

(2) **CIWIN by predstavovala systém rýchleho varovania (RAS), ktorý by zabezpečoval prepojenie členských štátov s Komisiou.** Táto možnosť by zvýšila bezpečnosť najdôležitejšej infraštruktúry zabezpečením varovaní obmedzených na bezprostredné hrozby a varovania. Cieľom by v tomto prípade bolo zjednodušenie rýchlej výmeny informácií o možných ohrozeniach pre majiteľov a prevádzkovateľov najdôležitejšej infraštruktúry. Systém rýchleho varovania by nezahŕňal poskytovanie dlhodobého spravodajstva. Využíval by sa na rýchle poskytnutie informácií o bezprostredných ohrozeniach špecifickej infraštruktúry.

(3) **CIWIN by bola viacúrovňovým komunikačným/varovným systémom plniacim dve rôzne funkcie:** a) systém rýchleho varovania, ktorý by zabezpečoval prepojenie

členských štátov s Komisiou a b) fórum pre výmenu návrhov a osvedčených postupov v súvislosti s ochranou najdôležitejšej infraštruktúry na podporu majiteľov a prevádzkovateľov najdôležitejšej infraštruktúry, pozostávajúce zo siete expertov a platformy pre elektronickú výmenu údajov.

Bez ohľadu na vybratú možnosť by CIWIN dopĺňala existujúce siete a vynaložilo by sa všetko úsilie na zabránenie duplicity. Z dlhodobého hľadiska by CIWIN mohla byť napojená na všetkých príslušných majiteľov a prevádzkovateľov v každom členskom štáte, napríklad prostredníctvom národného koordinačného orgánu pre ochranu najdôležitejšej infraštruktúry. Varovania a osvedčené postupy by bolo možné sprostredkúvať prostredníctvom tohto orgánu, ktorý by bol jediným subjektom priamo napojeným na Komisiu a tým na všetky ostatné členské štáty. Na vytvorenie národnej odnože CIWIN, spájajúcej orgány s konkrétnymi majiteľmi a prevádzkovateľmi, by členské štáty mohli využiť svoje súčasné informačné systémy. Podstatné je, že tieto národné siete by mohli využívať príslušné orgány ochrany najdôležitejšej infraštruktúry členských štátov a majitelia a prevádzkovatelia ako dvojsmerný komunikačný systém.

Zrealizuje sa štúdia na určenie rozsahu a technických špecifikácií potrebných na budúce rozhranie CIWIN s členskými štátmi.

**Otázky**

Akú formu by mala mať CIWIN, aby prispievala k cieľom EPCIP?

Mali by byť na CIWIN prepojení majitelia a prevádzkovatelia najdôležitejšej infraštruktúry?

### 9.2. Spoločná metodika

Rôzne členské štáty majú rôzne úrovne varovania na rôzne situácie. V súčasnosti nie je možné odhadnúť, či napríklad pojem „vysoký“ v jednom členskom štáte znamená to isté ako v inom členskom štáte. Nadnárodným spoločnostiam to môže skomplikovať určenie priorít v rámci výdavkov na ochranné opatrenia. Preto by pokus o zjednotenie alebo rovnakú kalibráciu jednotlivých úrovní varovania mohol znamenať prínos.

Pre každú úroveň ohrozenia by mohla existovať úroveň pripravenosti umožňujúca spustenie spoločných ochranných opatrení vo všeobecných prípadoch a prípadne špecifických ochranných opatrení v osobitných prípadoch. Členské štáty, ktoré nechcú uplatňovať niektoré opatrenie, by mohli riešiť špecifickú hrozbu alternatívnymi bezpečnostnými opatreniami.

Mohla by sa zvážiť spoločná metodika na určenie a zatriedenie hrozieb, možností reakcií, rizík a zraniteľných miest a vypracovanie záverov o možnosti, pravdepodobnosti a stupni závažnosti, ktorú ohrozenie predstavuje pre porušenie zariadenia infraštruktúry. To by zahŕňalo hodnotenie rizika a stanovenie priorít, v rámci ktorých by rizikové udalosti mohli byť definované pokiaľ ide o pravdepodobnosť ich vzniku, dosahu a vzťahu k ostatným rizikovým oblastiam a procesom.

**Otázky**

Do akej miery je potrebné a reálne zjednotiť alebo kalibrovať rôzne úrovne varovaní?

Mala by existovať spoločná metodika na určenie a zatriedenie hrozieb, možností reakcií, rizík a zraniteľných miest a vypracované závery o možnosti, pravdepodobnosti a stupni závažnosti, ktorú ohrozenie predstavuje?

### 9.3. Financovanie

Na základe iniciatívy Európskeho parlamentu (vytvorenie novej rozpočtovej položky v rozpočte na rok 2005 – pilotný projekt „Boj proti terorizmu“, Komisia 15. septembra prijala rozhodnutie o alokovaní 7 miliónov eur na financovanie súboru opatrení, ktoré posilnia európsku prevenciu, pripravenosť a reakciu na teroristické útoky vrátane riadenia následkov, ochrany najdôležitejšej infraštruktúry, ako aj opatrení súvisiacich s financovaním terorizmu, výbušnín a násilnej radikalizácie. Viac než dve tretiny tohto rozpočtu sú určené na prípravu budúceho Európskeho programu na ochranu najdôležitejšej infraštruktúry, zapojenie a rozvoj kapacít potrebných na riadenie kríz nadnárodného významu, ktoré vyplývajú z potenciálnych teroristických útokov a núdzové opatrenia, ktoré môžu byť potrebné na reakciu voči vážnemu ohrozeniu alebo výskytu takéhoto útoku. Predpokladá sa, že financovanie bude v roku 2006 pokračovať.

V priebehu rokov 2007 až 2013 bude financovanie zabezpečené prostredníctvom rámcového programu o bezpečnosti a ochrane slobôd. To zahŕňa aj osobitný program o „Prevencii, pripravenosti a riadení následkov terorizmu“. Komisia navrhla alokovať 137,4 milióna eur na určenie príslušných potrieb a vypracovanie spoločných technických noriem na ochranu najdôležitejšej infraštruktúry.

Program umožní poskytnutie finančných prostriedkov Spoločenstva na projekty predložené vnútroštátnymi, regionálnymi a miestnymi orgánmi na ochranu najdôležitejšej infraštruktúry. Program sa zameriava na určenie potrieb ochrany a poskytovanie informácií s cieľom vypracovania spoločných noriem a hodnotenia ohrození a rizík pre potreby ochrany najdôležitejšej infraštruktúry alebo vypracovanie špecifických pohotovostných plánov. Komisia by využila svoje súčasné odborné znalosti alebo by mohla podporiť financovanie štúdií o vzájomných závislostiach v špecifických sektoroch. Je potom najmä na zodpovednosti členských štátov alebo majiteľov a prevádzkovateľov, aby zdokonalili bezpečnosť svojej infraštruktúry podľa definovaných potrieb. Samotný program nefinancuje zdokonalenie ochrany najdôležitejšej infraštruktúry. Na zdokonalenie ochrany infraštruktúry v členských štátoch podľa potrieb definovaných v programe a na zavedenie spoločných noriem by sa mohli využiť pôžičky z finančných inštitúcií. Komisia by bola ochotná podporiť sektorové štúdie na hodnotenie finančného dopadu, ktorý by zdokonalenie ochrany infraštruktúry mohlo mať na priemysel.

Komisia financuje výskumné projekty na podporu ochrany najdôležitejšej infraštruktúry v rámci prípravnej činnosti na výskum v oblasti bezpečnosti[2] (2004 – 2006) a vo svojom návrhu rozhodnutia Rady a Európskeho parlamentu týkajúceho sa Siedmeho rámcového

[2] Celková výška úverov v rozpočte na rok 2004 a na rok 2005 dosiahla 30 miliónov eur. Na rok 2006 Komisia navrhla sumu 24 miliónov eur, ktorá je v súčasnosti predmetom preskúmania zo strany rozpočtového orgánu.

programu pre výskum (KOM(2005)119, konečné znenie)[3] a návrhu rozhodnutia Rady týkajúce sa osobitného programu „Spolupráca“, ktorým sa implementuje Siedmy rámcový program, pripravila významnejšie činnosti pre výskum v oblasti ochrany. Cieľovo orientovaný výskum, ktorého cieľom je poskytnúť praktické stratégie alebo nástroje na zníženie rizika, má v rámci ochrany najdôležitejšej infraštruktúry EÚ v strednodobom až dlhodobom meradle najvyššiu dôležitosť. Všetky bezpečnostné výskumy vrátane výskumov v tejto oblasti sa predložia na preskúmanie z etickej stránky, aby sa zabezpečil súlad s Chartou základných práv. Potreba výskumu sa zvýši pri náraste počtu vzájomných závislostí infraštrukúry.

**Otázky**

Ako by ste odhadli náklady a dosah implementácie opatrení predkladaných v tejto Zelenej knihe na administratívu a priemysel? Myslíte si, že je to zodpovedajúce?

### 9.4. Hodnotenie a monitorovanie

Hodnotenie a monitorovanie implementácie EPCIP predstavuje viacúrovňový proces, ktorý si vyžaduje zapojenie všetkých zainteresovaných subjektov:

- **na úrovni EÚ by sa mohol zaviesť mechanizmus vzájomného hodnotenia**, v rámci ktorého by členské štáty a Komisia spoločne pracovali na hodnotení celkovej úrovne implementácie EPCIP v každom členskom štáte. Komisia by mohla vypracovávať ročné správy o pokroku v implementácii EPCIP,

- **Komisia by každý kalendárny rok podávala správu o pokroku členským štátom a ostatným orgánom** v rámci pracovného dokumentu útvarov Komisie,

- **na úrovni členských štátov by celkovú implementáciu EPCIP v rámci príslušnej jurisdikcie na dodržiavanie súladu s národným(-i) programom(-ami) na ochranu najdôležitejšej infraštruktúry a sektorovými programami na ochranu najdôležitejšej infraštruktúry mohol monitorovať Národný koordinačný orgán pre ochranu najdôležitejšej infraštruktúry každého členského štátu**, prostredníctvom ročných správ podávaných Rade a Komisii, aby sa zabezpečila ich účinná implementácia.

Implementácia EPCIP by predstavovala dynamický, neustále sa vyvíjajúci proces, ktorý je potrebné hodnotiť, aby sa udržal krok s najnovším vývojom vo svete a využili získané skúsenosti. Vzájomné hodnotenia a monitorovacie správy členských štátov by mohli patriť medzi nástroje revízie EPCIP a navrhovania nových opatrení na posilnenie ochrany najdôležitejšej infraštruktúry.

Príslušné informácie členských štátov o najdôležitejšej infraštruktúre EÚ by sa mohli sprístupniť Komisii na vypracovanie spoločného hodnotenia zraniteľných miest, plánov riadenia následkov, spoločných noriem ochrany najdôležitejšej infraštruktúry, stanovenie priorít vo výskumnej činnosti, prípadne reguláciu a harmonizáciu. Takéto informácie by boli utajované a uchovávané ako prísne dôverné.

---

[3] Návrh rozpočtu Komisie na výskumné činnosti súvisiace s bezpečnosťou a vesmírom v rámci Siedmeho programu pre výskum a technologický rozvoj (RTD) predstavuje 570 miliónov eur (KOM(2005)119, konečné znenie).

Komisia by mohla monitorovať rôzne iniciatívy členských štátov vrátane tých, u ktorých sa predpokladajú finančné dôsledky pre majiteľov a prevádzkovateľov, ktorí nedokážu obnoviť základné služby pre občanov v stanovenom maximálnom časovom rámci.

**Otázka**

Aký druh hodnotiaceho mechanizmu by bol potrebný pre EPCIP? Bol by vyššie uvedený mechanizmus postačujúci?

Odpovede zasielajte v elektronickej forme do 15. januára 2006 na e-mailovú adresu: **JLS-EPCIP@cec.eu.int**. S odpoveďami sa bude zaobchádzať ako s dôvernými materiálmi, pokiaľ odosielateľ vyslovene neuvedie, že si praje, aby sa uverejnili. V takom prípade ich Komisia umiestni na svoju internetovú stránku.

**ANNEXES**

**ANNEX 1**

## CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

**Alert**

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

**Critical infrastructure protection (CIP)**

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

**Critical Information Infrastructure (CII):**

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

**Critical Information Infrastructure Protection (CIIP)**

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

**Contingency plan**

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

**Critical Information**

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

**Critical Infrastructure (CI)**

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

**Essential service**

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

**European critical infrastructure (ECI)**

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

**Impact**

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  - Environment (effect on the public and surrounding location);

  - Interdependency (between other critical infrastructure elements).

  - Political effects (confidence in the ability of government);

  - Psychological effects (may escalate otherwise minor events). both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

**Interdependency**

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

**Occurrence**

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

**Operator Security Plan**

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

**Prevention**

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

**Response**

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

**Risk**

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

**Threat**

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

**Vulnerability**

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

**ANNEX 2**

## INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

| Sector | | Product or service | |
|---|---|---|---|
| I | Energy | 1 | Oil and gas production, refining, treatment and storage, including pipelines |
| | | 2 | Electricity generation |
| | | 3 | Transmission of electricity, gas and oil |
| | | 4 | Distribution of electricity, gas and oil |
| II | Information, Communication Technologies, ICT | 5 | Information system and network protection |
| | | 6 | Instrumentation automation and control systems (SCADA etc.) |
| | | 7 | Internet |
| | | 8 | Provision of fixed telecommunications |
| | | 9 | Provision of mobile telecommunications |
| | | 10 | Radio communication and navigation |
| | | 11 | Satellite communication |
| | | 12 | Broadcasting |
| III | Water | 13 | Provision of drinking water |
| | | 14 | Control of water quality |
| | | 15 | Stemming and control of water quantity |
| IV | Food | 16 | Provision of food and safeguarding food safety and security |
| V | Health | 17 | Medical and hospital care |
| | | 18 | Medicines, serums, vaccines and pharmaceuticals |
| | | 19 | Bio-laboratories and bio-agents |
| VI | Financial | 20 | Payment services/payment structures (private) |
| | | 21 | Government financial assignment |
| VII | Public & Legal Order and Safety | 22 | Maintaining public & legal order, safety and security |
| | | 23 | Administration of justice and detention |
| VIII | Civil administration | 24 | Government functions |
| | | 25 | Armed forces |
| | | 26 | Civil administration services |
| | | 27 | Emergency services |
| | | 28 | Postal and courier services |
| IX | Transport | 29 | Road transport |
| | | 30 | Rail transport |
| | | 31 | Air traffic |
| | | 32 | Inland waterways transport |
| | | 33 | Ocean and short-sea shipping |
| X | Chemical and nuclear industry | 34 | Production and storage/processing of chemical and nuclear substances |
| | | 35 | Pipelines of dangerous goods (chemical substances) |
| XI | Space and Research | 36 | Space |
| | | 37 | Research |

**ANNEX 3**

**OPERATOR SECURITY PLAN**

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

***Introduction)***

Contains information concerning the pursued objectives and the main organisational and protection principles.

***Detailed part*** *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- Graduated security measures, which may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.