EUROOPA ÜHENDUSTE KOMISJON

Brüssel 17.11.2005
KOM(2005) 576 lõplik

ROHELINE RAAMAT

EUROOPA ESMATÄHTSA INFRASTRUKTUURI KAITSE PROGRAMMI KOHTA

(komisjoni esitatud)

ROHELINE RAAMAT

EUROOPA ESMATÄHTSA INFRASTRUKTUURI KAITSE PROGRAMMI KOHTA

1. TAUST

Esmatähtsat infrastruktuuri võidakse kahjustada, see purustada või selle toimimist häirida tahtlike terroriaktide, loodusõnnetuste, hooletuse, õnnetuste või arvutihäkkerluse, kriminaalse tegevuse või kuritahtliku käitumisega. ELis terrorismi, loodusõnnetuste ja õnnetuste tõttu ohtu seatud inimelude ja inimeste vara päästmiseks peaks esmatähtsa infrastruktuuri mis tahes toimimise häiritus või sellega manipuleerimine olema võimalikult lühiajaline, harvaesinev, hallatav, geograafiliselt isoleeritud ja liikmesriikide, nende kodanike ja Euroopa Liidu heaolu võimalikult vähe kahjustav. Hiljutised terrorirünnakud Madridis ja Londonis on selgelt välja toonud Euroopa infrastruktuuri vastu suunatud terrorirünnakute ohu. ELi reaktsioon peab olema kiire, kooskõlastatud ja tõhus.

Euroopa Ülemkogu palus 2004. aasta juulis komisjonil koostada üldstrateegia esmatähtsa infrastruktuuri kaitseks. Vastusena sellele võttis komisjon 20. oktoobril 2004. aastal vastu teatise "Esmatähtsa infrastruktuuri kaitse terrorismivastases võitluses", milles ta esitas konkreetsed soovitused selle kohta, kuidas tõhustada esmatähtsate infrastruktuuridega seotud terrorirünnakute ennetamist, nendeks valmisolekut ja nendele reageerimist Euroopas.

Nõukogu järeldused "Terrorirünnakute ennetamine, nendeks valmisolek ja nendele reageerimine" ning "ELi solidaarsusprogramm terroriähvarduste ja -rünnakute tagajärgede kohta", mille nõukogu võttis vastu 2004. aasta detsembris, toetasid komisjoni kavatsust teha ettepanek Euroopa esmatähtsa infrastruktuuri kaitse programmiks (EPCIP - *European Programme for the Protection of Critical Infrastructure*) ning neis nõustuti sellega, et komisjon loob esmatähtsa infrastruktuuri hoiatusinfovõrgu (CIWIN - *Critical Infrastructure Warning Network*).

Komisjon on korraldanud kaks seminari ja kutsunud liikmesriike üles pakkuma välja ideesid ja esitama kommentaare. Esimene ELi esmatähtsa infrastruktuuri kaitse seminar toimus 6.–7. juunil 2005. aastal, millel osalesid liikmesriigid. Seminari järel esitasid liikmesriigid komisjonile asjakohased tausta käsitlevad dokumendid oma lähenemisviisi kohta esmatähtsa infrastruktuuri kaitsele ja kommenteerisid seminaril arutatud ideesid. Arvamusavaldused saadi juunis ja juulis ning need võeti aluseks esmatähtsa infrastruktuuri kaitse edasiarendamisel. Teine ELi esmatähtsa infrastruktuuri kaitse seminar peeti 12.–13. septembril, et arutelu esmatähtsa infrastruktuuri kaitse küsimustes edasi viia. Sellel seminaril osalesid nii liikmesriigid kui tööstusliidud. Selle tulemusena on komisjon otsustanud esitada käesoleva rohelise raamatu, milles on välja toodud erinevad EPCIP võimalused.

2. ROHELISE RAAMATU EESMÄRK

Rohelise raamatu peamine eesmärk on saada tagasisidet võimalike EPCIP poliitiliste valikute kohta, kaasates suurel arvul huvirühmi. Esmatähtsa infrastruktuuri tõhus kaitse nõuab riigi ja ELi tasandil teabevahetust, kooskõlastamist ja koostööd kõigi huvitatud poolte

(infrastruktuuri omanikud ja haldajad, seadusandjad, kutseorganisatsioonid ja tööstusliidud) vahel koostöös kõigi valitsustasandite ja avalikkusega.

Rohelises raamatus on toodud võimalused, kuidas komisjon võib vastata nõukogu nõudmisele EPCIP ja CIWINi loomiseks, ja see kujutab endast Euroopa esmatähtsa infrastruktuuri kaitse programmi väljatöötamisega seonduva konsultatsiooniprotsessi teist etappi. Komisjon ootab käesoleva rohelise raamatu esitamise järel konkreetset tagasisidet käesolevas dokumendis kirjeldatud poliitiliste valikute kohta. Olenevalt konsultatsiooniprotsessi tulemustest võidakse 2006. aastal välja pakkuda EPCIP meetmepakett.

3. EPCIP EESMÄRK JA KOHALDAMISALA

3.1. EPCIP üldine eesmärk

EPCIP eesmärk oleks tagada esmatähtsa infrastruktuuri piisav ja võrdsetasemeline turvalisus, toimimishäirete miinimumini viimine ja kiire, läbiproovitud taastamise korraldamine kogu Euroopa Liidus. Kaitsetase ei pea kõigi esmatähtsate infrastruktuuride puhul tingimata sama olema ja võib oleneda mõjudest, mida esmatähtsa infrastruktuuri toimimishäired põhjustavad. EPCIP oleks pidev protsess ning vajalik on selle korrapärane läbivaatamine, et pidada sammu uute küsimuste ja probleemidega.

EPCIP peaks võimalikult suures ulatuses minimeerima mis tahes negatiivsed mõjud, mida suurendatud investeeringud turvalisusse võivad avaldada konkreetse tööstusharu konkurentsivõimele. Kulude proportsionaalsuse arvutamisel ei tohi unustada turgude stabiilsuse säilitamise vajadust, mis on hädavajalik pikaajaliste investeeringute puhul, ega mõju, mis turvalisusel on aktsiaturgude arengule ja makromajanduslikule mõõtmele.

Küsimus

Kas see on EPCIP jaoks asjakohane eesmärk? Kui mitte, siis milline peaks eesmärk olema?

3.2. Mille eest peaks EPCIP kaitsma?

Kuigi tagajärgede likvideerimise meetmed on enamiku toimimishäirete puhul samad või analoogsed, võivad kaitsemeetmed olenevalt ohu laadist erineda. Ohtude hulka, mis vähendaksid märkimisväärselt suutlikkust tagada elanikkonna põhivajadused ja ohutus, pidada korda ja osutada minimaalseid hädavajalikke avalikke teenuseid või tagada majanduse normaalne toimimine, võivad kuuluda tahtlikud rünnakud ja loodusõnnetused. Võimalused on järgmised:

a) **kõiki ohte võrdselt käsitlev lähenemisviis** – see oleks kõikehõlmav lähenemisviis, milles võetaks võrdselt arvesse nii tahtlike rünnakute ohtu kui loodusõnnetusi. See tagaks kaitsemeetmete vahelise sünergia maksimaalse ära kasutamise, kuid selles ei pandaks spetsiaalset rõhku terrorismile;

b) **kõiki ohte käsitlev lähenemisviis terrorismi prioriteediga** – see oleks paindlik lähenemisviis, mis tagaks seose muud liiki ohtudega, nagu tahtlike rünnakute ja loodusõnnetuste oht, kuid mille puhul prioriteediks oleks seatud terrorism. Kui kaitsemeetmete tase mingis tööstusharus leitakse olevat piisav, keskenduksid huvirühmad neile ohtudele, mille suhtes nad on veel haavatavad;

c) **terrorismiohtude lähenemisviis** – see oleks terrorismile keskendunud lähenemisviis, mille puhul ei pööratks tavalisematele ohtudele erilist tähelepanu.

Küsimus
Millise lähenemisviisi peaks EPCIP võtma? Miks?

4. ETTEPANEKUKOHASED KESKSED PÕHIMÕTTED

Tehakse ettepanek, et EPCIP aluseks võiksid olla järgmised kesksed põhimõtted:

- **Subsidiaarsus** – subsidiaarsus oleks EPCIPs kesksel kohal, sest esmatähtsa infrastruktuuri kaitse on eelkõige riigi enda kohustus. Põhiline vastutus esmatähtsa infrastruktuuri kaitse eest langeks liikmesriikidele ja omanikele/haldajatele, kes tegutsevad ühises raamistikus. Komisjon omalt poolt keskenduks aspektidele, mis on seotud selliste esmatähtsate infrastruktuuride kaitsega, millel on ELis piiriülene mõju. Omanike ja haldajate vastutus ja kohustus teha oma varade kaitseks ise otsused ja plaanid ei tohiks muutuda.

- **Täiendavus** – ühine EPCIP raamistik täiendaks olemasolevaid meetmeid. Kui ühenduse mehhanismid on juba paigas, tuleks nende kasutamist jätkata ja need peaksid aitama tagada EPCIP üldise rakendamise.

- **Konfidentsiaalsus** – esmatähtsa infrastruktuuri kaitsega seonduv teabevahetus peaks toimuma usalduse ja konfidentsiaalsuse õhkkonnas. See on vajalik, pidades silmas, et esmatähtsa infrastruktuuri varade kohta käivaid spetsiifilisi andmeid võidakse kasutada esmatähtsa infrastruktuuri rajatistele toimimishäirete või vastuvõetamatute tagajärgede põhjustamiseks. Esmatähtsa infrastruktuuri kaitse alane teave peaks nii ELi kui liikmesriikide tasandil olema salastatud ja ligipääsu peaks sellele võimaldama üksnes teadmisvajaduse põhjal.

- **Huvirühmade koostöö** – kõigil huvirühmadel, sh liikmesriikidel, komisjonil, tööstus- ja ettevõtlusühendustel, standardimisasutustel ning omanikel, haldajatel ja kasutajatel (kasutajatena mõistetakse organisatsioone, kes kasutavad infrastruktuuri äritegevuse ja teenuste osutamise eesmärgil), on esmatähtsa infrastruktuuri kaitses oma roll. Kõik huvirühmad peaksid tegema koostööd ja andma oma panuse EPCIP arendamisse ja rakendamisse vastavalt oma spetsiifilistele rollidele ja kohustustele. Liikmesriikide ametiasutused peaksid juhtima ja kooskõlastama oma jurisdiktsioonis asuva esmatähtsa infrastruktuuri kaitset käsitleva riigisiseselt ühtse lähenemisviisi väljatöötamist ja rakendamist. Omanikud, haldajad ja kasutajad oleksid aktiivselt kaasatud nii riigi kui ELi tasandil. Kui majandusharu standardid puuduvad või kui rahvusvahelisi norme ei ole veel kehtestatud, võiksid standardimisasutused ühised standardid vastu võtta, kui see on asjakohane.

- **Proportsionaalsus** – kaitsestrateegiad ja -meetmed oleksid kaasneva ohutasemega proportsionaalsed, sest kõiki infrastruktuure ei saa kaitsta kõigi ohtude eest (näiteks elektri ülekandevõrgud on liiga suured, et neile saaks tara ümber ehitada või neid valvata). Asjakohaste riskijuhtimistehnikate kohaldamise abil keskendataks tähelepanu kõige suurema riskiga valdkondadele, võttes arvesse ohtu, suhtelist esmatähtsust, kulude ja tulude suhet, turvalisuse taset ja olemasolevate leevendusstrateegiate tõhusust.

Küsimus

Kas need kesksed põhimõtted on vastuvõetavad? Kas mõned neist on üleliigsed? Kas on täiendavaid põhimõtteid, mida peaks arvesse võtma?

Kas nõustute sellega, et kaitsemeetmed peaksid olema kaasneva ohutasemega proportsionaalsed, sest kõiki infrastruktuure ei saa kõigi ohtude eest kaitsta?

5. ÜHINE EPCIP RAAMISTIK

Mõne infrastruktuuri kahjustada saamisel või hävimisel ühes liikmesriigis võib olla negatiivne mõju mitmetele teistele liikmesriikidele ja Euroopa majandusele tervikuna. See muutub üha tõenäolisemaks, sest uued tehnoloogiad (nt Internet) ja turgude liberaliseerimine (nt elektri ja gaasitarne puhul) tähendab, et paljud infrastruktuurid on osaks laiemast võrgustikust. Sellises olukorras on kaitsemeetmed vaid nii tugevad, kui tugev on nende nõrgim lüli. See tähendab, et vajalik võib olla ühtne kaitsetase.

Tõhus kaitse nõuab kõigi huvirühmade teabevahetust, kooskõlastamist ja koostööd riigi, ELi (kui see on asjakohane) ja rahvusvahelisel tasandil. Võiks paika panna ühise ELi tasandi raamistiku esmatähtsa infrastruktuuri kaitseks Euroopas tagamaks, et iga liikmesriik kaitseb oma esmatähtsat infrastruktuuri piisaval ja võrdsel tasemel ja et konkurentsieeskirju siseturul ei moonutata. Liimesriikide tegevuste toetamise eesmärgil toetaks komisjon esmatähtsa infrastruktuuri kaitsega seonduvate küsimuste alaste parimate tavade määratlemist, vahetamist ja levitamist, pakkudes esmatähtsa infrastruktuuri kaitse jaoks ühist raamistikku. Nimetatud üldise raamistiku ulatust on vaja kaaluda.

Ühine EPCIP raamistik hõlmaks horisontaalmeetmeid, millega määratletakse kõigi esmatähtsa infrastruktuuri huvirühmade pädevus ja kohustused ning millega pandaks alus majandusharupõhistele lähenemisviisidele. Ühine raamistik on mõeldud täienduseks olemasolevatele ühenduse tasandi ja liikmesriikide majandusharupõhistele meetmetele, et tagada Euroopa Liidus paiknevate esmatähtsate infrastruktuuride maksimaalne võimalik turvalisuse tase. Prioriteediks peaks seadma töö kokkuleppele jõudmiseks ühise mõistete ja esmatähtsate infrastruktuuride majandusharude loetelu suhtes.

Kuna esmatähtsat infrastruktuuri sisaldavad majandusharud on väga erinevad, oleks raske täpselt ette näha, milliseid kriteeriume peaks nende kõigi määramiseks ja kaitsmiseks horisontaalses raamistikus kasutama; seda peaks tegema majandusharude kaupa eraldi. Sellele vaatamata on vaja jõuda ühisele arusaamale teatavates valdkondadevahelistes küsimustes.

Seepärast soovitatakse saavutada esmatähtsate infrastruktuuride tugevdamine ELis ühise EPCIP raamistiku loomise (ühised eesmärgid ja metoodika nt võrdlemiseks, vastastikuste sõltuvuste leidmiseks), parimate tavade vahetamise ja täitmise jälgimise mehhanismidega. Mõned ühise raamistiku hulka kuuluvad elemendid oleksid:

- ühised esmatähtsate infrastruktuuride kaitse põhimõtted;
- ühiselt kokkulepitud eeskirjad/standardid;
- ühised määratlused, mille alusel saab kokku leppida valdkonnapõhistes määratlustes (soovituslik määratluste nimekiri on esitatud 1. lisas);
- ühine esmatähtsate infrastruktuuride majandusharude nimekiri (soovituslik majandusharude nimekiri on esitatud 2. lisas);

- esmatähtsa infrastruktuuri kaitse prioriteetsed valdkonnad;
- asjaomaste huvirühmade kohustuste kirjeldus;
- kokkulepitud võrdlusnäitajad;
- metoodika infrastruktuuride võrdlemiseks ja prioritiseerimiseks erinevates majandusharudes.

Selline raamistik minimeeriks ka võimalikke moonutavaid mõjusid siseturul.

Ühine EPCIP raamistik võiks olenevalt küsimusest olla kas vabatahtlik, kohustuslik või nende segu. Mõlemat liiki raamistikud aitaksid kaasa olemasolevatele majandusharupõhistele ja horisontaalsetele meetmetele ühenduse ja liikmesriikide tasandil; samas annaks ainult õiguslik raamistik tugeva ja jõustatava õigusliku aluse ELi esmatähtsate infrastruktuuride kaitse meetmete järjekindlaks ja ühesuguseks rakendamiseks ning määratleks selgelt liikmesriikide ja komisjoni vastavad ülesanded. Mittesiduvad vabatahtlikud meetmed oleksid küll paindlikud, kuid ei annaks selgust selles, kes mida teeb.

Olenevalt hoolika analüüsi tulemustest ja pöörates nõuetekohaselt tähelepanu ettepaneku kohaste meetmete proportsionaalsusele, võib komisjon oma EPCIP ettepanekus kasutada mitmeid vahendeid, sealhulgas õigusakte. Kui see on asjakohane, lisatakse spetsiifiliste meetmete ettepanekutele mõju hindamised.

Küsimused

Kas ühine raamistik oleks esmatähtsa infrastruktuuri kaitse tugevdamiseks tõhus?

Kui oleks vajalik õiguslik raamistik, siis milliseid elemente peaks see sisaldama?

Kas nõustute sellega, et ELi esmatähtsate infrastruktuuride eri liikide määratlemise kriteeriumid ja vajalikuks peetavad kaitsemeetmed peaks määratlema majandusharude kaupa eraldi?

Kas ühine raamistik aitaks kaasa asjaomaste huvirühmade kohustuste selgitamisele? Mil määral peaks selline ühine raamistik olema kohustuslik ja mil määral vabatahtlik?

Milline peaks olema ühise raamistiku kohaldamisala? Kas nõustute I lisas esitatud soovituslike mõistete ja määratluste nimekirjaga, mille alusel saab (kui see on asjakohane) luua majandusharupõhised määratlused? Kas nõustute II lisas esitatud esmatähtsate infrastruktuuride majandusharude nimekirjaga?

6. ELI ESMATÄHTSAD INFRASTRUKTUURID

6.1. ELi esmatähtsa infrastruktuuri määratlus

Selle, mis kujutab endast ELi esmatähtsat infrastruktuuri, saaks määratleda juhtumi piiriülese mõju kaudu, mis näitab, kas sellel võiks olla tõsine mõju väljaspool selle liikmesriigi territooriumi, kus rajatis paikneb. Teine punkt, mida peaks siin arvesse võtma, on asjaolu, et liikmesriikide vahelised kahepoolsed esmatähtsa infrastruktuuri kaitse alase koostöö skeemid kujutavad endast hästi sissetöötatud ja tõhusat vahendit esmatähtsa infrastruktuuriga tegelemiseks piiriüleselt kahe liikmesriigi vahel. Selline koostöö täiendaks EPCIPd.

ELi esmatähtsa infrastruktuuri hulka kuuluksid sellised füüsilised vahendid, teenused, infotehnoloogia rajatised, võrgud ja infrastruktuuri varad, mille toimehäiretel või hävitamisel oleks tõsine mõju tervisele, turvalisusele, julgeolekule, majanduslikule või sotsiaalsele heaolule:

a) kahes või enamas liikmesriigis – **see hõlmaks teatavaid kahepoolseid esmatähtsaid infrastruktuure (kui see on asjakohane)**;

b) kolmes või enamas liikmesriigis – **see hõlmaks kõiki kahepoolseid esmatähtsaid infrastruktuure.**

Nende võimaluste vastavaid eeliseid kaaludes on oluline silmas pidada järgmist:

– asjaolu, et mõni infrastruktuur on määratud ELi esmatähtsaks infrastruktuuriks, ei tähenda tingimata, et see vajaks täiendavaid kaitsemeetmeid. Olemasolevad kaitsemeetmed, mille hulka võivad kuuluda liikmesriikide vahelised kahepoolsed kokkulepped, võivad olla täiesti piisavad ja jäävad seega ELi esmatähtsaks infrastruktuuriks määramisel muutumatuks;

– valikuga a võib kaasneda rohkem ELi esmatähtsaks infrastruktuuriks määramisi;

– valik b võib tähendada, et infrastruktuuri puhul, mis on oluline ainult kahele liimesriigile, ei oleks ühendusel mingit rolli ka siis, kui üks neist kahest liikmesriigist peab kaitstuse taset ebapiisavaks ja teine liikmesriik keeldub samme astumast. Valik b võib viia ka rohkearvuliste liikmesriikide vaheliste kahepoolsete kokkulepete ja erimeelsusteni. Tööstusel, mis sageli toimib üleeuroopalisel tasandil, võib osutuda vajalikuks töötada erinevate kokkulepete rägastikus, mis võib kaasa tuua täiendavaid kulusid.

Peale selle tunnistatakse, et kaaluda tuleks ka väljastpoolt ELi pärinevaid või seal paiknevaid esmatähtsaid infrastruktuure, mis on aga ELi liikmesriigiga seotud või millel võib olla sellele otsene mõju.

Küsimus

Kas ELi esmatähtis infrastruktuur peaks olema infrastruktuur, millel võib olla tugev piiriülene mõju kahes või enamas liikmesriigis või kolmes või enamas liikmesriigis? Miks?

6.2. Vastastikune sõltuvus

Kõigi ELi esmatähtsate infrastruktuuride järkjärgulisel kindlakstegemisel soovitatakse eriti arvesse võtta vastastikuseid sõltuvusi. Vastastikuste sõltuvuste uurimine aitaks kaasa konkreetsete esmatähtsate infrastruktuuride vastu suunatud ohtude võimaliku mõju hindamisele ja aitaks eelkõige kindlaks teha, millised liimesriigid saaksid kahju esmatähtsate infrastruktuuridega seotud suurõnnetuse korral.

Täiel määral tuleks arvesse võtta ettevõtete, tööstusharude, geograafiliste võimkondade ja liikmesriikide ametiasutuste – eelkõige nende, kes kasutavad side- ja infotehnoloogiat – vastastikust sõltuvust. Komisjon, liikmesriigid ja esmatähtsate infrastruktuuride omanikud/haldajad töötaksid koos, et teha need vastastikused sõltuvused kindlaks ja kohaldada asjakohaseid strateegiaid riski vähendamiseks, kui see on võimalik.

Küsimus

Kuidas saab vastastikuseid sõltuvusi arvesse võtta?

Kas oskate välja pakkuda sobivaid metoodikaid vastastikuste sõltuvuste analüüsiks?

Millisel tasandil peaks vastastikuste sõltuvuste kindlakstegemine toimuma, kas ELi ja/või liikmesriigi tasandil?

6.3. ELi esmatähtsate infrastruktuuride rakendamise etapid

Komisjon soovitaks ELi esmatähtsate infrastruktuuride rakendamiseks järgimisi etappe:

(1) komisjon koostab koos liikmesriikidega konkreetsed kriteeriumid, mida kasutada ELi esmatähtsate infrastruktuuride kindlakstegemiseks majandusharu põhiselt;

(2) liikmesriigid ja komisjon teevad kindlaks ja kinnitavad järjest ELi esmatähtsad infrastruktuurid majandusharu põhiselt. Otsus teatava esmatähtsa infrastruktuuri määramiseks ELi esmatähtsaks infrastruktuuriks tehakse asjaomase infrastruktuuri piiriülese laadi tõttu Euroopa Liidu tasandil;[1]

(3) liikmesriigid ja komisjon analüüsivad ELi esmatähtsa infrastruktuuriga seonduvaid turvalisuse puudujääke majandusharude kaupa eraldi;

(4) liikmesriigid ja komisjon lepivad kokku meetmete võtmisel prioriteetsetes majandusharudes/infrastruktuurides, võttes arvesse vastastikuseid sõltuvusi;

(5) kui see on asjakohane, lepivad komisjon ja liikmesriigi põhilised huvirühmad iga majandusharu puhul kokku minimaalse kaitsetaseme meetmete ettepanekutes, mille hulka võivad kuuluda standardid;

(6) need meetmed rakendatakse pärast seda, kui nõukogu on ettepanekud vastu võtnud;

(7) liikmesriigid ja komisjon tagavad regulaarse jälgimise. Kui see on asjakohane, tehakse muudatus (meetmetes ja esmatähtsate infrastruktuuride määramises).

Küsimused

Kas ELi esmatähtsate infrastruktuuride rakendamise etappide loetelu on vastuvõetav?

Kuidas võiksid komisjon ja liikmesriigid ELi esmatähtsaid infrastruktuure määrata (liikmesriikidel on ekspertteadmised, komisjonil aga ülevaade Euroopa huvidest)? Kas see peaks olema õiguslik otsus?

Kas on vajadust vahekohtumehhanismi järele juhuks, kui mõni liikmesriik ei nõustu tema jurisdiktsiooni jäävat infrastruktuuri ELi esmatähtsaks infrastruktuuriks nimetama?

Kas on vajadust määramiste kinnitamiseks? Kelle kohustus see peaks olema?

[1] Välja arvatud riigikaitsega seotud infrastruktuuride puhul.

Kas liikmesriigil peaks olema võimalik määrata teises liikmesriigis või kolmandas riigis asuv infrastruktuur enda jaoks esmatähtsaks? Kuidas tuleks tegutseda, kui liikmesriik, kolmas riik või tööstus peab mõnda liikmesriigis asuvat infrastruktuuri enda jaoks esmatähtsaks?

Kuidas tuleks tegutseda, kui see liikmesriik ei pea seda esmatähtsaks? Kas on vaja kaebuste mehhanismi? Kui jah, siis millist?

Kas haldajal peaks olema võimalus kaebuse esitamiseks, kui ta ei nõustu oma määramise või määramata jätmisega? Kui jah, siis kellele?

Milline metoodika oleks vaja välja töötada meetmete võtmisel prioriteetsete majandusharude/infrastruktuuride määramiseks? Kas on juba olemas sobiv metoodika, mida saaks Euroopa tasandi jaoks kohandada?

Milline peaks olema komisjoni roll ELi esmatähtsa infrastruktuuriga seonduvate turvalisuse puudujääkide analüüsimisel?

7. RIIKLIKUD ESMATÄHTSAD INFRASTRUKTUURID

7.1. Riiklike esmatähtsate infrastruktuuride roll EPCIPs

Paljud Euroopa Liidu ettevõtted tegutsevad piiriüleselt ja nende suhtes kohaldatakse seetõttu riiklike esmatähtsate infrastruktuuridega seoses erinevaid kohustusi. Seepärast tehakse liikmesriikide ja ELi kui terviku huvides ettepanek, et iga liikmesriik kaitseb oma riiklikku esmatähtsat infrastruktuuri ühise raamistiku raames, et omanikud ja haldajad kõikjal Euroopas saaksid kasu sellest, et nende suhtes ei kohaldata erinevate raamistike rägastikku, millest tulenevad rohkearvulised metoodikad ja lisakulud. Seda silmas pidades teeb komisjon ettepaneku, et kuigi EPCIP puhul on põhiliselt keskendutud ELi esmatähtsale infrastruktuurile, ei saa riiklikku esmatähtsat infrastruktuuri sellest täielikult kõrvale jätta. Sellele vaatamata võib ette näha kolm võimalust:

a) riiklikud esmatähtsad infrastruktuurid on täielikult EPCIPsse integreeritud;

b) riiklikud esmatähtsad infrastruktuurid jäävad EPCIP kohaldamisalast välja;

c) liikmesriigid võivad EPCIP osi soovi korral kasutada siseriiklike esmatähtsate infrastruktuuride jaoks, kuid ei ole kohustatud seda tegema.

Küsimus

Esmatähtsa infrastruktuuri tõhus kaitse Euroopa Liidus näib nõudvat nii ELi esmatähtsa infrastruktuuri kui riikliku esmatähtsa infrastruktuuri kindlakstegemist. Kas nõustute sellega, et kuigi EPCIP peaks keskenduma ELi esmatähtsale infrastruktuurile, ei saa riiklikku esmatähtsat infrastruktuuri täielikult välja jätta?

Milline neist võimalustest on EPCIP jaoks kõige asjakohasem?

7.2. Riiklikud esmatähtsa infrastruktuuri kaitse programmid

Ühise EPCIP raamistiku alusel saaksid liikmesriigid oma riiklike esmatähtsate infrastruktuuride jaoks välja töötada riiklikud esmatähtsa infrastruktuuri kaitse programmid. Liikmesriikidel oleks võimalik kohaldada rangemaid meetmeid kui EPCIPs esitatud.

Küsimus

Kas see on soovitatav, et iga liikmesriik võtaks vastu EPCIPl põhineva riikliku esmatähtsa infrastruktuuri kaitse programmi?

7.3. Ühtne järelevalveasutus

Tõhususe ja ühtsuse vajadust silmas pidades oleks vaja, et iga liikmesriik määraks ühtse järelevalveasutuse, kes tegeleks kogu EPCIP rakendamisega. Ette võib näha kaks võimalust:

a) ühtne esmatähtsa infrastruktuuri kaitse järelevalveasutus;

b) riiklik kontaktasutus, millel puuduvad volitused, jättes korraldamise liikmesriikidele endile.

Selline asutus saaks EPCIP rakendamist oma jurisdiktsioonis kooskõlastada, jälgida ja selle üle järelevalvet teostada ning võiks olla komisjoni, teiste liikmesriikide ning esmatähtsate infrastruktuuride omanike ja haldajate jaoks peamine kontaktasutus esmatähtsa infrastruktuuri kaitse küsimustes. Nimetatud asutus võiks olla aluseks riiklikule esindatusele esmatähtsa infrastruktuuri kaitse küsimustega tegelevates ekspertgruppides ja võiks olla seotud esmatähtsa infrastruktuuri hoiatusinfovõrguga (CIWIN). Riiklik esmatähtsa infrastruktuuri kaitse kooskõlastusasutus võiks kooskõlastada riiklikke esmatähtsa infrastruktuuri kaitse küsimusi olenemata sellest, kas liikmesriigis juba on teisi asutusi või üksusi, mis on esmatähtsa infrastruktuuri kaitse küsimustega seotud.

Riiklike esmatähtsate infrastruktuuride järkjärgulise kindlakstegemise võiks saavutada nii, et kohustada infrastruktuuride omanikke ja haldajaid teavitama riiklikku esmatähtsa infrastruktuuri kaitse kooskõlastusasutust igasugusest asjakohasest esmatähtsate infrastruktuuride kaitsega seotud äritegevusest.

Riikliku esmatähtsa infrastruktuuri kaitse kooskõlastusasutuse kohustuseks võiks olla õigusliku otsuse tegemine tema jurisdiktsiooni kuuluva infrastruktuuri määramiseks riiklikuks esmatähtsaks infrastruktuuriks. See teave jääks ainuüksi asjaomase liikmesriigi käsutusse.

Erivolituste hulka võiksid kuuluda:

a) EPCIP üleüldise rakendamise kooskõlastamine, jälgimine ja järelevalve selle üle liikmesriigis;

b) esmatähtsa infrastruktuuri kaitse küsimustes peamiseks kontaktasutuseks olemine:

   i. komisjoni jaoks;

   ii. teiste liikmesriikide jaoks;

   iii. esmatähtsate infrastruktuuride omanike ja haldajate jaoks;

c) ELi esmatähtsa infrastruktuuri määramisel osalemine;

d) õigusliku otsuse tegemine tema jurisdiktsiooni kuuluva infrastruktuuri määramiseks riiklikuks esmatähtsaks infrastruktuuriks;

e) õiguskaitsevahendeid pakkuvaks ametiasutuseks olemine omanikele/haldajatele, kes ei nõustu sellega, et nende infrastruktuur määratakse esmatähtsaks infrastruktuuriks;

f) riikliku esmatähtsa infrastruktuuri kaitse programmi ja majandusharupõhiste esmatähtsa infrastruktuuri kaitse programmide valjatöötamises osalemine;

g) konkreetsete esmatähtsate infrastruktuuride majandusharude vastastikuste sõltuvuste kindlakstegemine;

h) esmatähtsa infrastruktuuri kaitse majandusharupõhistele lähenemisviisidele kaasaaitamine osalemise kaudu ekspertgruppides. Omanike ja haldajate esindajaid võiks kutsuda andma aruteludesse oma panust. Tuleks pidada regulaarseid koosolekuid;

i) järelevalve esmatähtsa infrastruktuuriga seonduvate kriisikavade koostamise üle.

Küsimused

Kas nõustute sellega, et riiklike esmatähtsate infrastruktuuride määramine ja haldamine ühise EPCIP raamistiku raames peaks olema üksnes liikmesriikide kohutus?

Kas on soovitav nimetada igas liikmesriigis riikliku esmatähtsa infrastruktuuri kooskõlastusasutus, millel on kogu vastutus esmatähtsa infrastruktuuri kaitsega seonduvate meetmete kooskõlastamise eest, respekteerides samas olemasolevaid majandusharupõhiseid kohustusi (tsiviillennundusasutused, Seveso direktiiv jms)?

Kas sellise kooskõlastusasutuse jaoks pakutud volitused on asjakohased? Kas on muid vajalikke volitusi?

7.4. Riiklike esmatähtsate infrastruktuuride rakendamise etapid

Komisjon soovitaks riiklike esmatähtsate infrastruktuuride rakendamiseks järgimisi etappe:

(1) liikmesriigid koostavad EPCIPd kasutades konkreetsed kriteeriumid, mida riiklike esmatähtsate infrastruktuuride kindlakstegemisel kasutada;

(2) liikmesriigid teevad kindlaks ja kinnitavad järjest riiklikud esmatähtsad infrastruktuurid majandusharu põhiselt;

(3) liikmesriigid analüüsivad riiklike esmatähtsate infrastruktuuridega seonduvaid turvalisuse puudujääke majandusharude kaupa eraldi;

(4) liikmesriigid panevad paika meetmete võtmisel prioriteetsed majandusharud, võttes arvesse vastastikuseid sõltuvusi ja kui see on asjakohane, siis ELi tasandil kokku lepitud prioriteete;

(5) kui see on asjakohane, lepivad liikmesriigid iga majandusharu puhul kokku minimaalsetes kaitsemeetmetes;

(6) liikmesriikide kohustuseks on tagada, et nende jurisdiktsiooni kuuluvad omanikud/haldajad viiksid vajalikud rakendusmeetmed ellu;

(7) liikmesriigid tagavad regulaarse jälgimise. Kui see on asjakohane, tehakse muudatusi (meetmetes ja esmatähtsate infrastruktuuride määramises).

Küsimus

Kas riiklike esmatähtsate infrastruktuuride rakendamise etappide loetelu on vastuvõetav? Kas mõni etapp on üleliigne? Kas mõni etapp tuleks lisada?

8. ESMATÄHTSATE INFRASTRUKTUURIDE OMANIKE, HALDAJATE JA KASUTAJATE ROLL

8.1. Esmatähtsate infrastruktuuride omanike, haldajate ja kasutajate kohustused

Esmatähtsa infrastruktuuri määramisest tulenevad omanikele ja haldajatele teatavad kohustused. Riiklikeks või ELi esmatähtsateks infrastruktuurideks määratud infrastruktuuride omanike ja haldajate jaoks võiks ette näha neli kohustust:

(1) **liikmesriigi asjaomase esmatähtsa infrastruktuuri kaitse asutuse teavitamine asjaolust, et infrastruktuur võib olla oma laadilt esmatähtis;**

(2) **kõrgema(te) esindaja(te) määramine, kes tegutseks turvalisuse kontaktametnikuna omaniku/haldaja ja liikmesriigi asjaomase esmatähtsa infrastruktuuri kaitse asutuse vahel.** Turvalisuse kontaktametnik osaleks turvalisuse tagamise ja kriisikavade väljatöötamisel. Turvalisuse kontaktametnik oleks liikmesriigis peamine kontaktametnik asjaomase esmatähtsa infrastruktuuri kaitse majandusharu asutuse jaoks ja kui see on asjakohane, siis õiguskaitseorganite jaoks;

(3) **haldaja turvalisuse tagamise kava koostamine, rakendamine ja ajakohastamine.** Ettepanekukohase haldaja turvalisuse tagamise kava vorm on esitatud 3. lisas.

(4) esmatähtsa infrastruktuuriga seonduva **kriisikava väljatöötamises osalemine** koos liikmesriigi asjaomaste kodaniku- ja õiguskaitseorganitega, kui see on nõutav.

Haldaja turvalisuse tagamise kava võiks riikliku esmatähtsa infrastruktuuri kaitse kooskõlastusasutuse üldise järelevalve all esitada heakskiitmiseks liikmesriigi asjaomasele esmatähtsa infrastruktuuri kaitse majandusharu ametiasutusele olenemata sellest, kas tegemist on riikliku või ELi esmatähtsa infrastruktuuriga, et tagada erinevate omanike ja haldajate ning üldisemalt asjaomaste majandusharude võetud turvameetmete ühtsus. Omanikele ja haldajatele peaks seevastu andma asjakohast tagasisidet ja toetust seoses asjakohaste ohtudega ning parimate tavade väljakujunemisega ning kui see on asjakohane, siis abi vastastikuste sõltuvuste ja nõrkade kohtade hindamisel riikliku esmatähtsa infrastruktuuri kaitse kooskõlastusasutuse kaudu ja kui see on asjakohane, siis komisjoni poolt.

Iga liikmesriik võiks seada riiklike ja ELi esmatähtsate infrastruktuuride omanikele ja haldajatele haldaja turvalisuse tagamise kava koostamiseks (ELi esmatähtsate infrastruktuuride korral oleks sellesse kaasatud ka komisjon) tähtaja ning võiks näha ette haldustrahvid olukordade jaoks, kus nimetatud tähtaegasid ei järgita.

Tehakse ettepanek määratleda haldaja turvalisuse tagamise kavas omaniku/haldaja esmatähtsa infrastruktuuri varad ja näha nende kaitseks ette asjakohased julgeolekulahendused. Haldaja turvalisuse tagamise kavas kirjeldataks meetodeid ja protseduure, mida tuleb järgida, et tagada vastavus EPCIPle, riiklikele esmatähtsa infrastruktuuri kaitse programmidele ja asjakohastele spetsiifilistele esmatähtsa infrastruktuuri kaitse programmidele. Haldaja turvalisuse tagamise kava võib esmatähtsa infrastruktuuri kaitse reguleerimisel kujutada endast vahendit altpoolt tuleva algatuse lähenemisviisi jaoks, millega antakse erasektorile suurem mänguruum (ja ühtlasi ka suurem vastutus).

Konkreetsetel juhtudel, kui tegemist on teatavate infrastruktuuridega nagu elektri jaotusvõrgud ja teabevõrgud, oleks (praktilisest ja rahalisest vaatepunktist lähtuvalt) ebarealistlik oodata, et omanikud ja haldajad tagaksid kõigi oma varade võrdse kaitstuse taseme. Sellistel juhtudel tehakse ettepanek, et omanikud ja haldajad võiksid koos asjaomaste ametiasutustega teha kindlaks füüsilise või teabevõrgu kriitilised punktid (sõlmpunktid), mille ümber turvalisuse kaitsemeetmed koondada.

Haldaja turvalisuse tagamise kavas esitatud turvameetmed võiksid olla organiseeritud kahe pealkirja ümber:

- **alalised turvameetmed,** mille all määrataks kindlaks hädavajalikud investeeringud turvalisusse ja vahendid, mida omanik/haldaja ei saa paigaldada lühiajalise etteteatamisega. Omanik/haldaja säilitaks pideva valvsuse võimalike ohtude suhtes, mis ei segaks tema tavapärast majanduslikku, halduslikku ja sotsiaalset tegevust;

- **astmelised turvameetmed,** mille saaks aktiveerida olenevalt erinevatest ohutasemetest. Haldaja turvalisuse tagamise kavas peaks seega olema ette nähtud erinevad turvarežiimid, mida saaks kohandada selles liikmesriigis eksisteerivate võimalike ohutasemetega, kus infrastruktuur paikneb.

Tehakse ettepanek, et kui esmatähtsa infrastruktuuri omanik ja haldaja ei täida haldaja turvalisuse tagamise kava väljatöötamise, kriisikavade väljatöötamises osalemise ja turvalisuse kontaktametniku määramise kohustust, siis sellega kaasneks rahatrahvi määramise võimalus.

Küsimused

Kas esmatähtsa infrastruktuuri omanike/haldajate võimalikud kohustused esmatähtsa infrastruktuuri turvalisuse suurendamisel on vastuvõetavad? Milline oleks nende tõenäoline maksumus?

Kas omanikud ja haldajad peaksid olema kohustaud teavitama asjaolust, et nende infrastruktuur võib olla oma laadilt esmatähtis? Kas arvate, et haldaja turvalisuse tagamise kava kontseptsioon on kasulik? Miks?

Kas ettepaneku kohased kohustused on kaasnevate kuludega proportsionaalsed?

Mis õigused võiksid liikmesriigid ja komisjon esmatähtsate infrastruktuuride omanikele ja haldajatele anda?

8.2. Dialoog esmatähtsate infrastruktuuride omanike, haldajate ja kasutajatega

EPCIP raames võiksid omanikud ja haldajad luua partnerlusi. Mis tahes kaitseprogrammi edu sõltub omanike ja haldajatega saavutatavast koostööst ja kaasatuse tasemest. Liikmesriikides võiksid esmatähtsate infrastruktuuride omanikud ja haldajad pideva kontakti hoidmise teel riikliku esmatähtsa infrastruktuuri kaitse kooskõlastamisasutusega olla tihedalt kaasatud esmatähtsate infrastruktuuride kaitse arengutesse.

ELi tasandil võiks luua foorumid, et lihtsustada vaadete vahetamist üldiste ja majandusharupõhiste esmatähtsate infrastruktuuride kaitse küsimuste kohta. Ühine lähenemisviis erasektori kaasamisele esmatähtsate infrastruktuuride kaitsega seonduvatesse küsimustesse, millega toodaks kokku kõik avaliku ja erasektori huvirühmad, annaks liikmesriikidele, komisjonile ja tööstusele olulise platvormi, mille kaudu pidada sidet mis tahes uue üleskerkinud esmatähtsate infrastruktuuride kaitse küsimuse kohta. Esmatähtsate infrastruktuuride omanikud, haldajad ja kasutajad saaksid aidata kaasa ühiste suuniste, parimate tavade standardite ja kui see on asjakohane, siis teabevahetuse väljatöötamisele. Selline dialoog aitaks kujundada EPCIP tulevasi läbivaatamisi.

Kui see on asjakohane, siis võiks komisjon soodustada ELi esmatähtsate infrastruktuuride kaitsega seotud tööstuse/ettevõtete ühenduste loomist. Kaks viimast eesmärki peaksid tagama Euroopa tööstuse konkurentsivõime säilitamise ja ELi kodanike turvalisuse suurenemise.

Küsimus

Kuidas peaks dialoog esmatähtsate infrastruktuuride omanike, haldajate ja kasutajatega olema struktureeritud?

Kes peaks omanikke, haldajaid ja kasutajaid avaliku ja erasektori dialoogis esindama?

9. EPCIP TOETUSMEETMED

9.1. Esmatähtsa infrastruktuuri hoiatusinfovõrk (CIWIN)

Komisjon on välja töötanud mitu kiirhoiatussüsteemi, mis võimaldavad konkreetset, kooskõlastatud ja tõhusat reageerimist hädaolukordade korral, sh nende korral, mis on seotud terrorismiga. 20. oktoobril 2004. aastal andis komisjon teada keskse infovõrgu loomisest komisjonis, millega tagatakse teabe kiire liikumine komisjoni kõigi kiirhoiatussüsteemide ja asjaomaste komisjoni talituste (ARGUS) vahel.

Komisjon paneb ette luua CIWIN, mis võiks stimuleerida asjakohaste katsemeetmete väljatöötamist, edendades parimate tavade turvalist vahetamist ning olles vahendiks, mille kaudu edastada teavet otseste ohtude ja hoiatuste kohta. Süsteem tagaks, et õigetel inimestel on õigel ajal kättesaadav õige teave.

CIWINi väljatöötamiseks on järgmised kolm võimalust:

(1) **CIWIN võtaks foorumi vormi, mis on piirdub esmatähtsa infrastruktuuri kaitse ideede ja parimate tavade vahetamisega,** toetades sellega esmatähtsate infrastruktuuride omanikke ja haldajaid. Selline foorum võiks olla korraldatud ekspertide võrgustikuna ja elektroonilise platvormina asjakohase teabe vahetamiseks turvalises keskkonnas. Komisjon mängiks sellise teabe kogumisel ja levitamisel olulist rolli. See võimalus ei võimaldaks vajalikku kiiret hoiatamist vahetute ohtude korral. Ette võiks aga näha CIWINi laiendamise tulevikus.

(2) **CIWIN oleks liikmesriike komisjoniga ühendav kiirhoiatussüsteem.** See võimalus suurendaks esmatähtsa infrastruktuuri turvalisust, võimaldades hoiatamist, mis piirduks vahetute ohtude ja hoiatustega. Eesmärgiks oleks siin lihtsustada teabe kiiret vahetamist esmatähtsa infrastruktuuri omanikke ja haldajaid ähvardavate võimalike ohtude kohta. Kiirhoiatussüsteem ei hõlmaks kaua kogutud teabe jagamist. Seda kasutataks kiireks teabe jagamiseks vahetute ohtude kohta kindlale infrastruktuurile.

(3) **CIWIN oleks mitmetasandiline teabevahetus/hoiatussüsteem, mis koosneks kahest erinevast funktsioonist:** a) liikmesriike ja komisjoni ühendav kiirhoiatussüsteem; b) foorum esmatähtsate infrastruktuuride kaitsega seonduvate ideede ja parimate tavade vahetamiseks, millega toetataks esmatähtsate infrastruktuuride omanikke ja haldajaid ning mis koosneks ekspertide võrgustikust ja elektroonilisest andmevahetusplatvormist.

Olenemata tehtud valikust oleks CIWIN täienduseks olemasolevatele võrgustikele ning nõuetekohaselt tuleks hoolitseda selle eest, et vältida kattumist. Pikaajaliselt võiks CIWINiga ühendada kõik asjaomased esmatähtsate infrastruktuuride omanikud ja haldajad igas liikmesriigis näiteks riikliku esmatähtsa infrastruktuuri kaitse kooskõlastusasutuse kaudu. Hoiatusi ja parimaid tavasid saaks edastada selle asutuse kaudu, mis oleks ainus talitus, mis on otseselt ühendatud komisjoniga ja selle kaudu kõigi liikmesriikidega. Liikmesriikidel oleks võimalik oma riigisisese CIWINi toimimisvõime tagamiseks kasutada oma olemasolevaid infosüsteeme, mis ühendavad ametiasutusi konkreetsete omanike ja haldajatega. Oluline on see, et liikmesriigi asjaomased esmatähtsate infrastruktuuride kaitse asutused ning omanikud ja haldajad saaksid neid riigisiseseid võrke kasutada kahesuunalise teabevahetussüsteemina.

Algatatakse uuring selleks, et kindlaks määrata ulatus ja tehnilised näitajad, mis on vajalikud CIWINi tulevase kasutajaliidese jaoks liikmesriikidega.

Küsimused

Millisel kujul peaks CIWINi võrgustik EPCIP eesmärkide toetamiseks olema?

Kas esmatähtsate infrastruktuuride omanikud ja haldajad peaksid olema CIWINiga ühendatud?

9.2. Ühised metoodikad

Erinevad liikmesriigid kasutavad erinevatele situatsioonidele reageerimiseks erinevaid häiretasemeid. Praegu ei ole kuidagi võimalik teada, kas "kõrge" ühes liikmesriigis tähendab sama, mis "kõrge" teises liikmesriigis. See võib muuta mitmes riigis tegutsevate ettevõtete jaoks raskeks oma kaitsemeetmete kulude prioritiseerimise. Seepärast võib olla kasulik püüda erinevaid tasemeid ühtlustada või kalibreerida.

Igale ohutasemele võiks vastata valmisoleku tase, mille alusel võib käivitada üldiselt ühised turvameetmed või kui see on asjakohane, siis konkreetsemalt astmeliste turvameetmete kasutamise. Liikmesriigil, kes ei soovi mõnda konkreetset meedet kasutada, oleks võimalik reageerida konkreetsele ohule alternatiivsete turvameetmetega.

Kaaluda võiks ühise metoodika kasutuselevõtmist ohtude, suutlikkuse, riskide ja nõrkade kohtade kindlakstegemiseks ja liigitamiseks ning järelduste tegemiseks selle kohta, kui võimalik, tõenäoline ja mis raskusastmega on infrastruktuuri rajatise toimimise häirituse oht. See hõlmaks riskireitingut ja prioritiseerimist, mille käigus riskijuhtumid määratletaks nende toimumise tõenäosuse, mõju ja seoste kaudu teiste riskivaldkondade või protsessidega.

Küsimused

Mil määral on erinevate häiretasemete ühtlustamine või kalibreerimine soovitav ja teostatav?

Kas peaks olema ühine metoodika ohtude, suutlikkuse, riskide ja nõrkade kohtade kindlakstegemiseks ja liigitamiseks ning järelduste tegemiseks selle kohta, kui võimalik, tõenäoline ja mis raskusastmega on oht?

9.3. Rahastamine

Euroopa Parlamendi algatuse järel (uue eelarverea loomine 2005. aasta eelarves – terrorismivastast võitlust käsitlev katseprojekt) võttis komisjon 15. septembril vastu otsuse 7 miljoni euro eraldamiseks meetmete rahastamiseks, mis võetakse terrorirünnakute ennetamiseks, nendeks valmisolekuks ja nendele reageerimiseks Euroopas ja mis hõlmavad tagajärgede likvideerimist, esmatähtsa infrastruktuuri kaitset ning meetmeid, mis seonduvad terrorismi rahastamise, lõhkeainete ja vägivaldse radikaliseerumisega. Üle kahe kolmandiku kõnealusest eelarvest on pühendatud tulevase Euroopa esmatähtsa infrastruktuuri kaitse programmi ettevalmistamiseks, võimalikest terrorirünnakutest tulenevate piiriülese mõjuga kriiside ohjamiseks nõutavate ressursside integreerimiseks ja arendamiseks ning hädaabimeetmeteks, mis võivad olla vajalikud märkimisväärsele ohule või sellisele rünnakule reageerimiseks. 2006. aastal oodatakse selle rahastamise jätkumist.

2007–2013 toimub rahastamine turvalisuse ja vabaduste kaitse raamprogrammist. Selle hulka kuulub terrorismi ennetamise, selleks valmisoleku ja selle tagajärgede ohjamise eriprogramm; komisjoni ettepanekuga eraldati 137,4 miljonit eurot selleks, et määrata kindlaks vastavad vajadused ja töötada esmatähtsa infrastruktuuri kaitseks välja ühised tehnilised standardid.

Programmi raames rahastab ühendus projekte, mille riiklikud, piirkondlikud ja kohalikud ametiasutused on esitanud esmatähtsate infrastruktuuride kaitseks. Programm keskendub kaitsevajaduste kindlakstegemisele ja teabe andmisele eesmärgiga töötada välja ühised standardid, ohu- ja riskihindamine, et kaitsta esmatähtsaid infrastruktuure või töötada välja spetsiaalsed kriisikavad. Komisjon kasutaks oma olemasolevaid ekspertteadmisi või võiks aidata rahastada konkreetsete majandusharude vastastikuste sõltuvuste kohta tehtavaid uuringuid. Kindlakstehtud vajaduste kohaselt on infrastruktuuride turvalisuse suurendamine peamiselt liikmesriikide või omanike ja haldajate kohustus. Programmist endast esmatähtsate infrastruktuuride kaitse suurendamist ei rahastata. Programmi raames kindlaks tehtud vajaduste kohaselt saaks liikmesriikides paikneva infrastruktuuri turvalisuse suurendamiseks ja ühiste standardite rakendamiseks kasutada finantsinstitutsioonidelt saadud laene. Komisjon oleks valmis toetama majandusharupõhiseid uuringuid, mille abil hinnata infrastruktuuri turvalisuse suurendamise võimalikke finantsmõjusid tööstusele.

Komisjon rahastab teadusprojekte esmatähtsa infrastruktuuri kaitse toetamiseks julgeolekualase teadustöö ettevalmistusmeetmete[2] (2004–2006) raames ja on planeerinud julgeolekualase teadustöö valdkonnas põhjalikumaid meetmeid oma ettepanekus nõukogu ja Euroopa Parlamendi otsuse tegemiseks seoses EÜ 7. teadusuuringute raamprogrammiga (KOM(2005)119 lõplik)[3] ja oma ettepanekus nõukogu otsuse tegemiseks seoses 7. raamprogrammi rakendamise eriprogrammiga "Koostöö" (KOM(2005)440 lõplik). Sihtuuringud, mille eesmärk on pakkuda välja praktilised strateegiad või vahendid riskide vähendamiseks, on ELi esmatähtsa infrastruktuuri turvalisuse tagamisel keskmises kuni pikemas perspektiivis esmajärgulise tähtsusega. Kõigi julgeolekualaste uuringute suhtes, ka käesolevas valdkonnas, kohaldatakse eetilist läbivaatamist, et tagada nende kooskõla inimõiguste hartaga. Nõudlus teadusuuringute järele kasvab, kui infrastruktuuride sõltuvused suurenevad.

Küsimused

Kuidas hindaksite käesolevas rohelises raamatus esitatud meetmete rakendamise maksumust ja mõju valitsusele ja tööstusele? Kas see on proportsionaalne?

---

2 2004. ja 2005. aasta eelarves oli krediidi kogusumma 30 miljonit eurot. 2006. aasta kohta on komisjon teinud ettepaneku, et see võiks olla 24 miljoni eurot, mida eelarvepädevad institutsioonid praegu läbi vaatavad.

3 Teadusuuringute ja tehnoloogia arenduse 7. raamprogrammi kuuluvate julgeoleku ja kosmoseuuringutega seonduvate meetmete kohta tehtud komisjoni eelarveettepaneku summa on 570 miljonit eurot (KOM(2005)119 lõplik).

9.4. Hindamine ja jälgimine

EPCIP rakendamise hindamiseks ja jälgimiseks võiks kasutada mitmetasandilist protsessi, mis nõuab kõigi huvirühmade kaasatust:

- **ELi tasandil võiks ette näha vastastikuse hindamise mehhanismi,** milles liikmesriigid ja komisjon teeksid koostööd EPCIP üleüldise rakendustaseme hindamisel igas liikmesriigis. Komisjon võiks EPCIP rakendamise kohta koostada iga-aastased arenguaruanded;

- **komisjon annaks aru edasiminekust liikmesriikidele ja teistele institutsioonidele igal kalendriaastal** komisjoni töödokumendis;

- **liikmesriikide tasandil võiks igas liikmesriigis asuv riiklik esmatähtsa infrastruktuuri kaitse kooskõlastusasutus jälgida EPCIP üleüldist rakendamist oma jurisdiktsioonis, tagades vastavuse riikliku (riiklike) esmatähtsa infrastruktuuri kaitse programmi(de)ga,** et tagada nende tegelik rakendamine ja esitada selle kohta nõukogule ja komisjonile iga-aastaselt aruanne.

EPCIP rakendamine oleks dünaamiline protsess, mis areneb pidevalt edasi ja mida hinnatakse pidevalt, et pidada muutuva maailmaga sammu ja areneda edasi saadud kogemuste baasilt. Vastastikune hindamine ja liikmesriikide jälgimisaruanded võiksid olla osa EPCIP läbivaatamiseks kasutatavatest vahenditest ning nende alusel saaks välja pakkuda uusi meetmeid esmatähtsa infrastruktuuri tugevdamiseks ja kaitseks.

Liikmesriigid võiksid muuta ELi esmatähtsa infrastruktuuri käsitleva asjakohase teabe komisjonile kättesaadavaks, et saaks välja töötada ühised nõrkade kohtade hindamised, tagajärgede likvideerimise plaanid, ühised esmatähtsa infrastruktuuri kaitse standardid, seades prioriteediks uurimistegevuse ja kui see on vajalik, siis regulatsiooni ja ühtlustamise. Selline teave oleks salastatud ja seda hoitaks rangelt konfidentsiaalsena.

Komisjon võiks jälgida liikmesriikide erinevaid algatusi, sealhulgas neid, millega nähakse ette finantstagajärjed omanike ja haldajate jaoks, kes ei suuda hädavajalikke teenuseid kindlaksmääratud maksimaalse aja jooksul kodanikele uuesti kättesaadavaks muuta.

Küsimus

Mis liiki hindamismehhanismi EPCIP jaoks vaja oleks? Kas eespool nimetatud mehhanism oleks piisav?

Vastused tuleks saata elektrooniliselt 15. jaanuariks 2006. aastal järgmisel e-posti aadressil: **JLS-EPCIP@cec.eu.int**. Neid hoitakse konfidentsiaalsena, välja arvatud juhul, kui vastaja kinnitab selgesõnaliselt, et ta soovib selle avalikustamist – sel juhul pannakse need üles komisjoni veebilehele.

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.