Sisäasiainministeriö E-KIRJELMÄ SM2007-00063

PEO Rajaniemi Kirsi 07.02.2007

EDUSKUNTA
Suuri valiokunta

Viite

Asia
Ehdotukset EU:n kriittisten infrastruktuurien suojeluohjelman perustamiseksi

U/E-tunnus: **EUTORI-numero:**

Ohessa lähetetään perustuslain 97 §:n mukaisesti Eduskunnalle Euroopan yhteisöjen komission 12 päivänä joulukuuta 2006 tekemä ehdotus neuvoston direktiiviksi Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä, komission tiedonanto elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta sekä näistä laadittu perusmuistio SM2007-00042.

Ehdotuksesta toimitetaan perustuslain 96 §:n mukainen selvitys mahdollisimman pikaisesti.

Neuvotteleva virkamies Jukka Metso

LIITTEET Perusmuistio SM2007-00042, KOM(2006)787 lopullinen (suomeksi ja ruotsiksi), SEK(2006) 1648 (suomeksi ja ruotsiksi), SEC(2006) 1654 (englanniksi), KOM(2006) 786 lopullinen (suomeksi ja ruotsiksi)

Asiasanat	pelastuspalvelu, oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, PLM, STM, TH, TM, VM, VNEUS

Sisäasiainministeriö PERUSMUISTIO SM2007-00042

PEO Metso Jukka 07.02.2007

Asia
EU; OSA; Ehdotukset EU:n kriittisten infrastruktuurien suojeluohjelman perustamiseksi

Kokous

Liitteet Viite

EUTORI/Eurodoc nro:

EU/2006/1763, EU/2006/1757

U-tunnus / E-tunnus:

Käsittelyn tarkoitus ja käsittelyvaihe:

Suomen kannan valmistelu;
Direktiiviehdotuksen ja tiedonannon käsittely on aloitettu neuvoston pelastuspalvelutyöryhmässä

Asiakirjat:

16932/06 PROCIV 272, KOM(2006) 786 lopullinen (komission tiedonanto)
16933/06 PROCIV 273, KOM(2006) 787 lopullinen (ehdotus neuvoston direktiiviksi)
16933/06 ADD1, SEK(2006) 1648 (vaikutusten arvioinnin tiivistelmä)
16933/06 ADD2, SEC(2006) 1654 (vaikutusten arviointi)

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

SEY 308 artikla ja Euratom 203 artikla, yksimielinen päätös, kuulemismenettely

Käsittelijä(t):

Jukka Metso, SM, p.160 42985
Erkki Hämäläinen, SM/KRP, p. 8388 6504
Mika Purhonen, Huoltovarmuuskeskus, p. 010 60 510 32
Mari Herranen, LVM, p. 160 28305
Hannu Mäntyvaara, UM, p. 160 55452
Mauri Valtonen, KTM, p. 160 64814
Kari Mäkinen, KTM, p. 160 63523
Olli Haikala, STM, p. 160 73214

Suomen kanta/ohje:

Yleistä

Suomi pitää hyvänä, että EU:ssa aloitetaan keskustelut kriittisen infrastruktuurin suojauksesta ja sen merkityksestä. Kriittinen infrastruktuuri ja esimerkiksi tieto- ja viestintäverkot ovat keskeisessä asemassa tämän päivän tietoyhteiskunnassa. Verkot eivät välttämättä noudata jäsenvaltioiden rajoja ja siten ongelma yhdessä EU:n jäsenvaltiossa aiheuttaa helposti ongelmia toisessa jäsenvaltiossa.

Suomi pitää komission esittämää lähestymistapaa hyvänä ja kannatettavana. Suomi pitää tärkeänä, että EU-tason kriittisten infrastruktuurien suojaamisohjelma on ohjeellinen, mutta kohteiden määrittely, nimeäminen ja suojaamistarpeen arviointi tehdään ja toteutetaan jäsenmaita velvoittavalla direktiivillä. Tällaisessa toteuttamistavassa tulee kuitenkin pitää huoli siitä, että direktiivillä ei säädellä itse suojeluohjelmaa.

Se, että EU-tason kriittiset infrastruktuurit tunnistetaan ja nimetään velvoittavalla säädöksellä, takaa jäsenmaiden kesken tasapuolisen ja yhtenäisen lähestymistavan ja käytännön. Jos vastaavat vaatimukset annettaisiin vain ohjeellisina, käytännöt eri jäsenmaissa todennäköisesti vaihtelisivat. Toimintatapoja, päätöksentekomenettelyä ja -rakennetta sekä täytäntöönpanoa koskevat säännökset vaativat kuitenkin vielä selkiyttämistä. Lisäksi jäsenmaille ja toiminnanharjoittajille asetettavia velvollisuuksia ja vaikutusmahdollisuuksia on kehitettävä ja vahvistettava.

Direktiiviehdotus

Suomi pitää direktiiviehdotusta lähtökohdiltaan hyvänä. Ehdotuksen yksityiskohdissa on kuitenkin paljon epäselviä ja tulkinnanvaraisia kohtia.

Yhteinen eurooppalainen lähestymistapa ja yhteiset periaatteet kriittisen infrastruktuurin suojaukseen on erittäin kannatettava ajatus. Kuitenkin toimintatavat ja päätöksenteko EU-tasoisten infrastruktuurien tunnistamiseksi, nimeämiseksi ja suojaustarpeen määrittelemiseksi vaativat tarkentamista, samoin kuin se, miten EU-tasoinen infrastruktuuri määritellään ja mihin määritelmä perustuu. Myös jäsenvaltioiden vaikutusmahdollisuudet päätöksenteossa ja toiminnanharjoittajan velvollisuudet vaativat erityistarkastelua.

Sektorikohtainen kriittisen infrastruktuurin suojauksen tarkastelu ja määrittely sekä tarpeiden analysointi on tarpeellista toteuttaa. Ehdotuksessa jää kuitenkin avoimeksi kysymys siitä, miten nämä horisontaaliset kriteerit laaditaan ja kenen toimesta. Myös luettelo painopistealoista sekä menettely luettelon muuttamiseksi on epäselvä.

Suomi kannattaa velvoitteita, jotka koskevat turvallisuussuunnitelmien laadintaa, ylläpitoa ja suunnitelmien toimittamista jäsenvaltion viranomaiselle sekä turvallisuusyhteyshenkilöiden nimeämistä. Ehdotuksen mukaan turvallisuusyhteyshenkilöt raportoivat sen maan viranomaiselle, jossa kyseinen infrastruktuuri sijaitsee, eivätkä suoraan komissiolle. Epäselvää on miten tässä asiassa toimitaan monikansallisten yritysten osalta.

Direktiivin säädökset eivät esitetyssä muodossa ole Suomelle pääosin ongelmallisia ja ne sisältyvät jo pitkälti kansalliseen lainsäädäntöön. Direktiivin antaminen näiden asioiden osalta on hyväksyttävää. Tärkeää on kuitenkin huomioida, että vastuu kansallisista infrastruktuureista on jäsenvaltioilla. Jäsenvaltioilla pitää siten olla oikeus ja mahdollisuus antaa tarkempia ja tiukempia säädöksiä, jos kansallinen tilanne niin vaatii.

Ehdotuksen mukaan eurooppalaisten infrastruktuurien määrittämisessä käytettävät kriteerit hyväksytään komiteamenettelyssä. Suomi suhtautuu tähän kriittisesti. Kriteerien määrittely voidaan nähdä teknisenä kysymyksenä, mutta kriittiseen infrastruktuuriin liittyen kriteerit voivat usein olla yhteiskunnallisia. Kriteerien määrittämisellä voi olla myös lainsäädännöllisiä vaikutuksia. Vähintäänkin tietyt peruskriteerit olisi annettava direktiivissä ja komiteamenettelyssä olisi kyse kriteerien täytäntöönpanosta.

Direktiiviehdotuksen mukaan komissio laatii ehdotuksen EU:n kriittisiä infrastruktuureja koskevaksi luetteloksi jäsenmaiden toimittamien tietojen ja muiden käytettävissään olevien tietojen pohjalta. Epäselväksi jää mitä nämä muut tiedot olisivat ja mikä olisi niiden merkitys suhteessa jäsenmaan antamiin tietoihin.

Suomi haluaa korostaa sitä, että kriittisten infrastruktuurien suojeluohjelmaan kytkeytyvät toiminnanharjoittajat edellyttävät luottamuksellisten tietojen turvaamista.

Suomen kantana on, että komission esittämä oikeusperusta (SEY 308 artikla ja Euratom 203) on ainoa mahdollinen, ja että neuvoston direktiivi on soveltuva säädöstyyppi.

Tiedonanto

Koska Suomi lukeutuu EU:n reuna-alueisiin, se pitää suojaamisohjelmaa ja sen ulkoista ulottuvuutta erittäin kannatettavana. Suojaamisohjelman ja etenkin toimialojen tunnistamisen yhteisellä lähestymistavalla ja toimeenpanolla edesautetaan sisämarkkinoiden toimivuutta ja yritysten kilpailukykyä EU:n sisällä.

Suomen näkemyksen mukaan on kannatettavaa, että tiedonannon sisältämän suojeluohjelman yleinen tarkoitus ja tavoite on parantaa kohteiden suojaamista perustumalla toissijaisuuteen, luottamuksellisuuteen, sidosryhmäyhteistyöhön ja alakohtaiseen lähestymistapaan. Suojaamisohjelman kolmiasteista toimintasuunnitelmaa tulee vielä kehittää asiantuntijatyöryhmien ja alakohtaisten kokemusten pohjalta. Toimintaohjelman keskeiset tavoitteet määrittää ja tunnistaa alakohtaisesti EU-tason infrastruktuurit, perustaa ja järjestää hallittu hälytys- ja tiedonsiirtojärjestelmä (CIWIN), valmiussuunnitelmat ja ulkoinen ulottuvuus ovat Suomen kannalta erityisen tärkeitä elementtejä.

Pääasiallinen sisältö:

Yleistä

Komissio antoi 12.12.2006 tiedonannon elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta ja direktiiviehdotuksen menettelystä Euroopan elintärkeiden infrastruktuurien määrittämiseksi. Ohjelman tarkoituksena on parantaa kriittisten infrastruktuurien suojaamista Euroopan unionissa. Direktiiviehdotuksen tavoitteena on sopia menettelytavoista miten elintärkeät infrastruktuurit tunnistetaan ja nimetään sekä yhteisestä lähestymistavasta niiden suojelun parantamiseksi.

Elintärkeillä (kriittisillä) infrastruktuureilla tarkoitetaan sellaisia omaisuuseriä tai niiden osia, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Euroopan kriittisellä infrastruktuurilla tarkoitetaan sellaisia kriittisiä infrastruktuureja, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi huomattavia seurauksia kahdessa tai useammassa jäsenvaltiossa tai vain yhdessä jäsenvaltiossa siinä tapauksessa, että kyseinen infrastruktuuri sijaitsee toisessa jäsenvaltiossa.

Suojaamisohjelman täytäntöönpano ja kehittäminen on tarkoitus toteuttaa sektorikohtaisesti. Komission ehdotuksessa sektoreita on 11: energia, ydinvoimateollisuus, tieto- ja viestintätekniikka, vesi, elintarvikkeet, terveydenhuolto, rahoituspalvelut, liikenne, kemianteollisuus, avaruus, tutkimuslaitteistot.

Kesäkuussa 2004 Eurooppa-neuvosto pyysi komissiota laatimaan kokonaisstrategian kriittisten infrastruktuurien suojaamiseksi. Tämän seurauksena komissio antoi lokakuussa 2004 tiedonannon ”Kriittisen infrastruktuurin suojelu terrorismin torjunnassa”. Tiedonannossa esitettiin, miten Euroopassa voitaisiin entistä paremmin ehkäistä kriittisiin infrastruktuureihin kohdistuvia terrori-iskuja sekä varautua ja reagoida niihin.

Neuvosto hyväksyi joulukuussa 2004 terrori-iskujen ehkäisemistä, niihin varautumista ja niihin reagoimista koskevat päätelmät sekä terroriuhkien ja -iskujen seurauksia koskevan EU:n yhteisvastuuohjelman. Samalla se antoi hyväksyntänsä komission aikomukselle esittää kriittisten infrastruktuurien suojaamista koskeva EU:n ohjelma ja perustaa kriittisten infrastruktuurien varoitusjärjestelmä (CIWIN).

Marraskuussa 2005 komissio antoi vihreän kirjan Euroopan elintärkeiden infrastruktuurien suojaamisohjelmasta. Siinä esitettiin vaihtoehtoja suojaamisohjelman ja varoitusjärjestelmän toteuttamista varten. Joulukuussa 2005 oikeus- ja sisäasioiden neuvosto kehotti kriittisten infrastruktuurien suojaamista koskevissa päätelmissään komissiota laatimaan ehdotuksen kriittisten infrastruktuurien suojaamista koskevaksi EU:n ohjelmaksi.

<u>Komission tiedonanto elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta (asiakirja 16932/06)</u>

Tiedonannossa esitellään kriittisten infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttamiseksi ehdotetut periaatteet, menettelyt ja välineet. Tarkoituksena on parantaa kriittisten infrastruktuurien suojaamista EU:ssa. Eri maissa asiat on toteutettu eri tavoin ja eritasoisesti joten ohjelmalla pyritään yhtenäistämään käytäntöjä.

Ensisijaisena ja alkuperäisenä uhkana oli terrorismi, mutta tsunami ja muiden suuronnettomuuksien kokemusten perusteella tarkoituksena on ottaa huomioon kaikentyyppiset onnettomuudet ja vaaratekijät.

Suojaamisohjelma perustuu kuuteen pääperiaatteeseen, jotka ovat toissijaisuus, täydentävyys, luottamuksellisuus, yhteistyö sidosryhmien kesken, oikeasuhteisuus ja alakohtainen lähestymistapa. Ohjelman toimintakehys käsittää seuraavat toimet:
– menettely kriittisten infrastruktuurien määrittämiseksi ja nimeämiseksi sekä yhteinen lähestymistapa tarvittavien suojaustoimenpiteiden arvioimiseksi (direktiiviehdotus)
– suojaamisohjelman toteuttamista koskeva toimintasuunnitelma
– kriittisten infrastruktuurien varoitusjärjestelmä (CIWIN)
– kriittisten infrastruktuurien suojaamista käsittelevät EU tason asiantuntijaryhmät
– kriittisten infrastruktuurien suojaamista koskevaan tietojenvaihtoon liittyvät menettelyt
– infrastruktuurien keskinäisten riippuvuussuhteiden määrittäminen ja analysointi
– jäsenvaltioiden tukeminen kansallisten kriittisten infrastruktuurien suojaamisessa asianomaisten jäsenvaltioiden pyynnöstä
– valmiussuunnitelmat
– toiminnan ulkoinen ulottuvuus.

Suojaamista varten jäsenmaiden tulisi perustaa EU-tason mekanismi, joka vastaa koordinoinnista ja yhteistyöstä. Tätä varten tarvitaan kuhunkin jäsenmaahan yhteyspisteet.

Kansallisten infrastruktuurien suojaaminen kuuluu ensisijaisesti niiden omistajille ja ylläpitäjille ja jäsenvaltiolle itselleen. Kansallisia infrastruktuureita määriteltäessä tulisi asianomaisten ottaa huomioon laadulliset ja määrälliset seuraukset. Tällaisia ovat laajuus, vakavuus, riippuvuussuhteet. Valmiussuunnittelu on keskeinen osa-alue, jonka tarkoituksena on minimoida aiheutuvat seuraukset.

Ehdotus neuvoston direktiiviksi Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta (asiakirja 16933/06)

Direktiiviehdotuksessa esitetään toimenpiteet, joiden avulla EU:n laajuiset infrastruktuurit voidaan nimetä ja määrittää sekä arvioida tarvetta parantaa niiden suojaamista.

Koska Euroopan kriittiset infrastruktuurit ulottuvat yli valtioiden rajojen, niiden tunnistamisessa ja nimeämisessä olisi EU:ssa hyvä olla yhdennetty menettely. Se myös edistäisi yhteistä turvallisuutta samoin kuin sisämarkkinoiden kykyä turvata yritystoiminnan kannattavuus. Vain yhteinen toimintakehys varmistaa sen, että toimenpiteitä toteutetaan johdonmukaisesti ja yhtenäisesti.

Infrastruktuurien tehokas suojaaminen edellyttää kaikkien sidosryhmien panostusta asiaan sekä kansallisella että EU-tasolla. EU:ssa on jo toteutettu suuri määrä alakohtaista sääntelyä, jolla on vaikutuksia suojaamisohjelmaan.

Erityisen oikeusperustaan puuttuessa direktiiviehdotus perustuu EY-sopimuksen 308 artiklaan ja Euratom-sopimuksen 203 artiklaan. Kumpikin artikla määrää samasta päätöksentekojärjestelmästä: neuvosto antaa säännökset yksimielisesti komission ehdotuksesta ja Euroopan parlamenttia kuultuaan. Komissio pyytää lausunnon myös Euroopan keskuspankilta.

Direktiiviehdotuksessa on 14 artiklaa. Sen keskeisiä osia ovat 2 artiklan määritelmät, 3 artiklan infrastruktuurien määrittäminen, 4 artiklan nimeäminen, 5 artiklan turvallisuussuunnitelmat, 6 artiklan turvallisuusyhteyshenkilö, 7 artiklan kansalliset uhkakuvat ja riskiselvitykset. Lisäksi 9 artiklan yhteyspisteet ja 10 artiklan suojaamistoimenpiteet luovat keskeisen toimintaympäristön.

Kansallinen käsittely:

Alustavia kantoja ovat antaneet keskeiset ministeriöt (mm. LVM, KTM, STM, UM, VM) sekä Huoltovarmuuskeskus. Jatkovalmistelussa selvitetään tarkemmin yksityisen sektorin kannat.

Eduskuntakäsittely:

Käsittely Euroopan parlamentissa:

Käsittelyä valiokunnassa (kansalaisvapaudet sekä oikeus- ja sisäasiat) ei ole vielä aloitettu.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

Direktiivin täytäntöönpano edellyttänee jonkin verran muutoksia sektorikohtaiseen lainsäädäntöön, lähinnä koskien yrityksille asetettavia suunnitteluvelvoitteita. Tarkempaa selvitystä sektorilainsäädännön täydennystarpeista ei ole kuitenkaan vielä tehty. Joillakin sektoreilla vastaavia velvoitteita on jo lainsäädännössä. Muun muassa teleoperaattorit ja rahoitusala ovat lakisääteisen varautumisen alaisia ja toimittavat raportit myös valvovalle viranomaiselle. Muilla sektoreilla on sopimusperusteisia suunnitteluvelvoitteita, esimerkiksi kaupan keskusliikkeet tekevät laajaa valmiustyötä ilman lakisääteistä velvoitetta.

Taloudelliset vaikutukset:

Ehdotuksella ei ole välittömiä vaikutuksia Suomen valtion talousarvioon.

Kansallisen yhteyspisteen tehtävät ovat uusia ja niistä seuraa mahdollisesti resurssitarvetta, jota ei ole kuitenkaan vielä pystytty arvioimaan.

Komission ehdotuksessa ei ole tarkemmin arvioitu kansallisille viranomaisille tai yksityiseen sektoriin kohdistuvia kustannusvaikutuksia. Komission on tarkoitus esittää kustannusarvioita sektorikohtaisten kriteerien määrittämisen yhteydessä.

EU ohjelman täytäntöönpanoa edistää osaltaan terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa koskeva rahoitusohjelma vuosille 2007–2013. Erityisohjelmasta voidaan rahoittaa kriittisten infrastruktuurien suojaamiseen liittyviä toimia, joita voidaan hyödyntää useissa EU:n jäsenvaltioissa. Näitä voisivat olla esimerkiksi erilaiset selvitys- ja analysointityöt ja pilottihankkeet.

Muut mahdolliset asiaan vaikuttavat tekijät:

Puheenjohtajamaa ei ole määrittänyt erityisiä aikataulutavoitteita ehdotusten käsittelylle. Komission ehdotukset esiteltiin neuvoston pelastuspalvelutyöryhmälle 19.12.2006 pidetyssä Suomen puheenjohtajakauden viimeisessä kokouksessa. Saksan puheenjohtajakaudella ehdotusten työryhmäkäsittely on aloitettu 29.1.2007. Käsittelyn pohjaksi puheenjohtaja on laatinut erillisen pääehdotuksia koskevan kysymyslistan. Komissio on toivonut, että direktiiviehdotus voitaisiin hyväksyä jo kesäkuussa 2007, mikä on kuitenkin hyvin epätodennäköistä. EU suojeluohjelma on kuitenkin mahdollisesti esillä 19.–20.4.2007 tai 12.–13.6.2007 oikeus- ja sisäasioiden neuvostossa.

Komissio on käynnistänyt sektorikohtaisen EU:n kriittisen infrastruktuurin tarkastelun. Komissio antoi 2.2.2007 energia- ja kuljetussektoria koskevan tiedonannon ja valmisteilla on lentoliikennettä (lentokenttiä) koskeva tiedonanto.

Komission on tarkoitus antaa alkuvuodesta 2008 päätösehdotus kriittisten infrastruktuurien varoitusjärjestelmän (CIWIN) perustamisesta.

Valtioneuvoston periaatepäätös yhteiskunnan elintärkeiden toimintojen turvaamisen strategiasta on perusajattelultaan samankaltainen kuin komission ehdotukset, muun muassa painopistealueet ovat samat – sähköinen infrastruktuuri ja energia. Myös valtioneuvoston asettamissa huoltovarmuuden yleisissä tavoitteissa on korostettu

yhteiskunnan teknisten perusrakenteiden merkitystä. Keväällä 2002 annetun valtioneuvoston päätöksen mukaiset huoltovarmuuden tavoitealat ovat yhteiskunnan tekniset perusrakenteet, kuljetus-, varastointi- ja jakelujärjestelmät, elintarvikehuolto, energiahuolto, sosiaali- ja terveydenhuolto sekä sotilaallista maanpuolustusta tukeva tuotanto ja järjestelmien ylläpito. Kansainvälistymisen, verkostoitumisen ja teknistymisen vuoksi varautumista yhteiskunnan kriittisiin teknisiin perusrakenteisiin kohdistuviin uhkiin ja riskeihin on lisätty.

Asiasanat	pelastuspalvelu, oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, PLM, STM, TH, TM, VM, VNEUS

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 12.12.2006
KOM(2006) 787 lopullinen

2006/0276 (CNS)

Ehdotus:

NEUVOSTON DIREKTIIVI

Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta

(komission esittämä)

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

PERUSTELUT

1) EHDOTUKSEN TAUSTA

- **Ehdotuksen perustelut ja tavoitteet**

Kesäkuussa 2004 kokoontunut Eurooppa-neuvosto pyysi komissiota laatimaan elintärkeiden infrastruktuurien suojaamista koskevan kokonaisstrategian. Komissio hyväksyi tämän vuoksi 20. lokakuuta 2004 tiedonannon ”Kriittisen infrastruktuurin suojelu terrorismin torjunnassa”. Tiedonannossa esitetään, miten Euroopassa voitaisiin entistä paremmin ehkäistä elintärkeisiin infrastruktuureihin kohdistuvia terrori-iskuja sekä varautua ja reagoida niihin.

Neuvosto hyväksyi joulukuussa 2004 terrori-iskujen ehkäisemistä, niihin varautumista ja niihin reagoimista koskevat päätelmät sekä terroriuhkien ja -iskujen seurauksia koskevan EU:n yhteisvastuuohjelman. Samalla se antoi hyväksyntänsä komission aikomukselle esittää elintärkeiden infrastruktuurien suojaamista koskeva EU:n ohjelma (European Programme for Critical Infrastructure Protection, EPCIP) ja perustaa elintärkeiden infrastruktuurien varoitusjärjestelmä (Critical Infrastructure Warning Information Network, CIWIN).

Marraskuussa 2005 komissio hyväksyi vihreän kirjan Euroopan elintärkeiden infrastruktuurien suojaamisohjelmasta. Siinä esitetään vaihtoehtoja suojaamisohjelman ja varoitusjärjestelmän toteuttamista varten.

Joulukuussa 2005 oikeus- ja sisäasioiden neuvosto kehotti komissiota laatimaan ehdotuksen elintärkeiden infrastruktuurien suojaamista koskevaksi EU:n ohjelmaksi kesäkuuhun 2006 mennessä.

Tässä direktiiviehdotuksessa esitetään komission ehdotukset toimenpiteistä, joiden avulla voidaan määrittää ja nimetä Euroopan elintärkeät infrastruktuurit ja arvioida tarvetta parantaa niiden suojaamista.

- **Yleinen tausta**

Euroopan unionissa on tiettyjä elintärkeitä infrastruktuureja, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi seurauksia kahdessa tai useammassa jäsenvaltiossa. On myös mahdollista, että jonkin jäsenvaltion alueella sijaitsevan elintärkeän infrastruktuurin toimintahäiriö aiheuttaa seurauksia jossakin toisessa jäsenvaltiossa. Tällaiset elintärkeät infrastruktuurit, joilla on valtioiden rajat ylittäviä vaikutuksia, olisi määritettävä ja nimettävä Euroopan elintärkeiksi infrastruktuureiksi (EEI). Tätä varten on otettava käyttöön yhteinen menettely, jonka avulla Euroopan elintärkeät infrastruktuurit voidaan määrittää ja arvioida tarvetta parantaa niiden suojaamista.

Koska elintärkeät infrastruktuurit ulottuvat yli valtioiden rajojen, niiden heikkouksien, haavoittuvuuden ja turvallisuusvajeiden kartoittamisessa olisi hyötyä koko EU:n laajuisesta yhdennetystä menettelystä, joka täydentäisi jäsenvaltioissa jo toteutettavia kansallisia suojaamisohjelmia ja toisi niille lisäarvoa. Tällainen menettely vahvistaisi myös EU:n sisämarkkinoiden kykyä turvata yritystoiminnan kannattavuus ja luoda vaurautta jatkuvalta pohjalta.

Eri toimialoilla on kertynyt erityistä kokemusta ja asiantuntemusta elintärkeiden infrastruktuurien suojaamisesta, ja ne asettavat myös omat vaatimuksensa tälle toiminnalle. Siksi elintärkeitä infrastruktuureja koskevan EU:n menettelyn suunnittelussa ja toteutuksessa olisikin otettava huomioon eri alojen erityisominaisuudet. Menettelyn tulisi perustua eri aloilla jo toteutettaviin elintärkeitä infrastruktuureja koskeviin toimenpiteisiin. Elintärkeistä infrastruktuurialoista on laadittava yhteinen luettelo, koska näin voidaan helpottaa elintärkeiden infrastruktuurien suojaamista koskevan alakohtaisen toimintamallin toteuttamista.

- **Tarvitaan yhteinen toimintakehys**

Vain yhteisen toimintakehyksen avulla voidaan varmistaa, että Euroopan elintärkeiden infrastruktuurien turvaamisen parantamiseen tähtääviä toimenpiteitä toteutetaan johdonmukaisesti ja yhtenäisesti. Näin voidaan myös määritellä selkeästi Euroopan elintärkeiden infrastruktuurien sidosryhmien vastuualueet. Vapaaehtoisuuteen perustuvien toimien etuna on joustavuus, mutta ne eivät anna työlle riittävän vakaata pohjaa. Jos toiminta perustuisi yksinomaan vapaaehtoisuuteen, tehtävänjako ei olisi kyllin selkeä eikä tilanne olisi liioin omiaan selkeyttämään Euroopan elintärkeisiin infrastruktuureihin liittyvien sidosryhmien oikeuksia ja velvollisuuksia.

Menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten ja yhteinen lähestymistapa niiden suojaamisen parantamistarpeiden arvioimista varten voidaan laatia vain direktiivin avulla. Näin voidaan varmistaa, että

- Euroopan elintärkeät infrastruktuurit on suojattu asianmukaisella tavalla;
- kaikkia Euroopan elintärkeiden infrastruktuurien sidosryhmiä koskevat samat oikeudet ja velvollisuudet;
- sisämarkkinoiden vakaus on turvattu.

Jonkin infrastruktuurin osan vaurioituminen tai tuhoutuminen yhdessä jäsenvaltiossa voi aiheuttaa ikäviä seurauksia monille muille jäsenvaltioille tai koko Euroopan talouselämälle. Tällaisen mahdollisuuden todennäköisyys kasvaa koko ajan, sillä huomattava osa infrastruktuurista on nivottu osaksi laajempaa verkkoa mm. uusien teknologioiden (esim. Internetin) ja markkinoiden vapautumisen myötä (esim. sähkön- ja kaasuntoimitukset). Tällaisessa tilanteessa suojaamistoimenpiteiden muodostama kokonaisuus on yhtä vahva kuin sen heikoin lenkki. Tämän vuoksi saattaa olla tarpeen turvata yhtäläinen suojauksen taso.

- **Alakohtainen vuoropuhelu sidosryhmien kesken**

Infrastruktuurien tehokas suojaaminen edellyttää kaikkien sidosryhmien keskinäistä viestintää, koordinointia ja yhteistyötä sekä kansallisella että EU:n tasolla.

On tärkeää saada yksityinen sektori täysipainoisesti mukaan toimintaan, sillä valtaosa elintärkeistä infrastruktuureista on yksityisomistuksessa ja niiden toiminta yksityisten talouden toimijoiden vastuulla. Jokaisen toimijan on vastattava omien riskiensä hallinnasta, sillä yleensä toimija tekee itsenäisesti päätöksen siitä, mitä suojaamistoimia se toteuttaa ja millaisia liiketoiminnan jatkuvuussuunnitelmia se soveltaa. Jatkuvuussuunnittelussa tulisi noudattaa tavanomaisia liiketoimintamenettelyjä ja -logiikkaa, ja ratkaisujen tulisi mahdollisuuksien mukaan perustua tavanomaisiin kaupallisiin järjestelyihin.

Eri toimialoilla on kertynyt erityistä kokemusta ja asiantuntemusta elintärkeiden infrastruktuurien suojaamisesta, ja toisaalta ne myös asettavat omat vaatimuksensa tälle toiminnalle.

Euroopan elintärkeiden infrastruktuurien suojaamisohjelmaa koskevaan vihreään kirjaan saatujen vastausten perusteella yksityinen sektori olisi saatava mukaan EU:n menettelyyn, jotta siinä voidaan ottaa huomioon eri alojen ominaispiirteet ja eri aloilla jo käytössä olevat suojaamistoimet.

- **Voimassa olevat aiemmat säännökset**

EU:n tasolla ei tähän mennessä ole annettu elintärkeiden infrastruktuurien suojaamista koskevia horisontaalisia säännöksiä. Tällä direktiivillä otetaan käyttöön menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteinen lähestymistapa niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten.

Eri aloilla on jo toteutettu seuraavat toimenpiteet:

- Tietotekniikka:

  a) Yleispalveludirektiivi (2002/22/EY), joka koskee mm. yleisten sähköisten viestintäverkkojen toimintakykyä

  b) Valtuutusdirektiivi (2002/20/EY), joka koskee mm. yleisten sähköisten viestintäverkkojen toimintakykyä

  c) Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY), joka koskee mm. yleisten sähköisten viestintäverkkojen turvallisuutta

  d) Neuvoston puitepäätös 2005/222/YOS, tehty 24 päivänä helmikuuta 2005, tietojärjestelmiin kohdistuvista hyökkäyksistä

  e) Asetus (EY) N:o 460/2004, annettu 10 päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta

- Terveydenhuolto:

  a) Euroopan parlamentin ja neuvoston päätös N:o 2119/98/EY, tehty 24 päivänä syyskuuta 1998, tartuntatautien epidemiologisen seurannan ja valvonnan verkoston perustamisesta yhteisöön

  b) Komission direktiivi 2003/94/EY, annettu 8 päivänä lokakuuta 2003, ihmisille tarkoitettujen lääkkeiden ja ihmisille tarkoitettujen tutkimuslääkkeiden hyvien tuotantotapojen periaatteista ja yleisohjeista

- Rahoitus:

  a) Euroopan parlamentin ja neuvoston direktiivi 2004/39/EY, annettu 21 päivänä huhtikuuta 2004, rahoitusvälineiden markkinoista

b) Europohjaisten vähittäismaksujärjestelmien valvontanormit, jotka Euroopan keskuspankin (EKP) hallintoneuvosto vahvisti kesäkuussa 2003

c) Euroopan parlamentin ja neuvoston direktiivi 2006/48/EY, annettu 14 päivänä kesäkuuta 2000, luottolaitosten liiketoiminnan aloittamisesta ja harjoittamisesta

d) Euroopan parlamentin ja neuvoston direktiivi 2006/49/EY, annettu 14 päivänä kesäkuuta 2006, sijoituspalveluyritysten ja luottolaitosten omien varojen riittävyydestä

e) Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi maksupalveluista sisämarkkinoilla ja direktiivien 97/7/EY, 2000/12/EY ja 2002/65/EY muuttamisesta (KOM(2005) 603)

f) Euroopan parlamentin ja neuvoston direktiivi 2000/46/EY, annettu 18 päivänä syyskuuta 2000, sähköisen rahan liikkeeseenlaskijoiden liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta

g) Euroopan parlamentin ja neuvoston direktiivi 1998/26/EY, annettu 19 päivänä toukokuuta 1998, selvityksen lopullisuudesta maksujärjestelmissä ja arvopaperien selvitysjärjestelmissä

- Liikenne:

a) Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004, annettu 31 päivänä maaliskuuta 2004, alusten ja satamarakenteiden turvatoimien parantamisesta

b) Komission asetus (EY) N:o 884/2005, annettu 10 päivänä kesäkuuta 2005, merenkulun turvaamisen alalla suoritettavissa komission tarkastuksissa noudatettavista menettelyistä

c) Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY, annettu 26 päivänä lokakuuta 2005, satamien turvallisuuden parantamisesta

d) Euroopan parlamentin ja neuvoston asetus (EY) N:o 2320/2002, annettu 16 päivänä joulukuuta 2002, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä

e) Komission asetus (EY) N:o 622/2003, annettu 4 päivänä huhtikuuta 2003, toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi

f) Komission asetus (EY) N:o 1217/2003, annettu 4 päivänä heinäkuuta 2003, kansallisia siviili-ilmailun turvaamisen laadunvalvontaohjelmia koskevista yhteisistä vaatimuksista

g) Komission asetus (EY) N:o 1486/2003, annettu 22 päivänä elokuuta 2003, siviili-ilmailun turvaamisen alalla suoritettavissa komission tarkastuksissa noudatettavista menettelyistä

h) Komission asetus (EY) N:o 68/2004, annettu 15 päivänä tammikuuta 2004, toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi annetun asetuksen (EY) N:o 622/2003 muuttamisesta

i) Euroopan parlamentin ja neuvoston asetus (EY) N:o 849/2004, annettu 29 päivänä huhtikuuta 2004, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä annetun asetuksen (EY) N:o 2320/2002 muuttamisesta

j) Komission asetus (EY) N:o 1138/2004, annettu 21 päivänä kesäkuuta 2004, lentoasemien turvavalvottujen alueiden kriittisten osien yhteisestä määritelmästä

k) Komission asetus (EY) N:o 781/2005, annettu 24 päivänä toukokuuta 2005, toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi annetun asetuksen (EY) N:o 622/2003 muuttamisesta

l) Komission asetus (EY) N:o 857/2005, annettu 6 päivänä kesäkuuta 2005, toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi annetun asetuksen (EY) N:o 622/2003 muuttamisesta

m) Euroopan parlamentin ja neuvoston direktiivi 2001/14/EY, annettu 26 päivänä helmikuuta 2001, rautateiden infrastruktuurikapasiteetin käyttöoikeuden myöntämisestä

n) Vaarallisten aineiden rautatiekuljetuksia säännellään direktiivillä 96/49/EY (sellaisena kuin se on muutettuna direktiivillä 2004/110/EY, uudet RID-määräykset tulevat voimaan vuonna 2005)

o) Yleissopimus ydinaineiden turvajärjestelyjä koskevista toimista (allekirjoitettu vuonna 1980, EU liittyi siihen vuonna 1981 ja sopimus tuli voimaan vuonna 1987)

- Kemianteollisuus:

a) Ns. Seveso II -direktiivissä tarkoitetut vaaralliset laitokset (neuvoston direktiivi 96/82/EY, annettu 9 päivänä joulukuuta 1996, vaarallisista aineista aiheutuvien suuronnettomuusvaarojen torjunnasta; direktiiviä on muutettu 16 päivänä joulukuuta 2003 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2003/105/EY)

- Ydinteollisuus:

    a) Neuvoston direktiivi 89/618/Euratom, annettu 27 päivänä marraskuuta 1989, säteilyvaaratilanteessa tarvittavia suojelutoimenpiteitä ja noudatettavia ohjeita koskevien tietojen antamisesta väestölle

    b) Neuvoston päätös 87/600/Euratom, tehty 14 päivänä joulukuuta 1987, yhteisön järjestelyistä nopeaksi tietojenvaihdoksi säteilyhätätilanteen yhteydessä.

- **Johdonmukaisuus suhteessa unionin muuhun politiikkaan ja muihin tavoitteisiin**

Ehdotus noudattaa täysin Euroopan unionin tavoitteita ja erityisesti tavoitetta, jonka mukaan unioni ”pitää yllä ja kehittää unionia vapauteen, turvallisuuteen ja oikeuteen perustuvana alueena, jossa henkilöiden vapaa liikkuvuus taataan toteuttamalla samalla ulkorajoilla tehtäviä tarkastuksia, turvapaikkaa, maahanmuuttoa sekä rikollisuuden ehkäisyä ja torjuntaa koskevat aiheelliset toimenpiteet”.

Ehdotus on johdonmukainen muiden politiikkojen kanssa, sillä sen tarkoituksena ei ole korvata voimassa olevia toimenpiteitä, vaan täydentää niitä niin, että Euroopan elintärkeiden infrastruktuurien suojaamista voidaan parantaa.

2) INTRESSITAHOJEN KUULEMINEN JA VAIKUTUSTEN ARVIOINTI

- **Intressitahojen kuuleminen**

Kaikkia elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman kannalta olennaisia sidosryhmiä on kuultu. Tätä varten on toteutettu seuraavat toimet:

- Euroopan elintärkeiden infrastruktuurien suojaamisohjelmaa koskeva vihreä kirja julkaistiin 17. marraskuuta 2005, ja kuulemismenettely päättyi 15. tammikuuta 2006. Kuulemisen yhteydessä esitettyihin kysymyksiin saatiin virallinen vastaus 22 jäsenvaltiolta. Lisäksi vihreään kirjaan saatiin kommentteja noin sadalta yksityisen sektorin toimijalta. Yleensä ottaen vastauksissa kannatetaan elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman perustamista.

- Komissio on järjestänyt kolme seminaaria, joissa on käsitelty elintärkeiden infrastruktuurien suojaamista (kesäkuussa 2005, syyskuussa 2005 ja maaliskuussa 2006). Kaikkiin seminaareihin osallistui edustajia eri jäsenvaltioista. Syyskuussa 2005 ja maaliskuussa 2006 pidettyihin seminaareihin kutsuttiin myös yksityisen sektorin edustajia.

- Elintärkeiden infrastruktuurien suojaamisen yhteyspisteiden epäviralliset tapaamiset. Komissio on järjestänyt jäsenvaltioiden yhteyspisteille kaksi tapaamista (joulukuussa 2005 ja helmikuussa 2006).

- Epäviralliset tapaamiset yksityisen sektorin edustajien kanssa. Useita epävirallisia tapaamisia on järjestetty myös yksittäisten yritysten sekä eri toimialajärjestöjen edustajien kanssa.

- Komission sisällä suojaamisohjelmaa on valmisteltu elintärkeiden infrastruktuurien suojaamista käsittelevän työryhmän säännöllisissä kokouksissa. Työryhmä on EU:n sisäistä terrorismia käsittelevän komission yksiköiden välisen työryhmän alaryhmä.

- **Asiantuntijatiedon käyttö**

Asiantuntijatietoa on koottu kokouksissa ja seminaareissa, joita järjestettiin vuosina 2004, 2005 ja 2006, sekä vihreään kirjaan perustuvan kuulemismenettelyn yhteydessä. Tietoja on kerätty kaikilta sidosryhmiltä, joita asia koskee.

- **Vaikutusten arviointi**

Tämän asiakirjan liitteenä on elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta laadittu vaikutustenarviointi.

3) EHDOTUKSEEN LIITTYVÄT OIKEUDELLISET NÄKÖKOHDAT

- **Ehdotetun toimen lyhyt kuvaus**

Ehdotetun toimen tarkoituksena on ottaa käyttöön horisontaalinen kehys Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä sekä niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten.

- **Oikeusperusta**

Ehdotuksen oikeusperusta on Euroopan yhteisön perustamissopimuksen 308 artikla.

- **Toissijaisuusperiaate**

Ehdotus on toissijaisuusperiaatteen mukainen, sillä jäsenvaltiot eivät voi yksinään toteuttaa siihen sisältyviä toimenpiteitä, vaan ne on toteutettava EU:n tasolla. Vaikka jokaisen jäsenvaltion on edelleen huolehdittava itse oman lainkäyttövaltansa piiriin kuuluvan elintärkeän infrastruktuurin turvaamisesta, Euroopan unionin turvallisuuden kannalta on erittäin tärkeää varmistaa, että infrastruktuuri, joka vaikuttaa kahteen tai useampaan jäsenvaltioon tai vain yhteen jäsenvaltioon siinä tapauksessa, että kyseinen infrastruktuuri sijaitsee toisessa jäsenvaltiossa, on suojattu riittävän hyvin ja että yksi tai useampi jäsenvaltio ei joudu alttiiksi häiriöille toisissa jäsenvaltioissa sijaitsevissa infrastruktuureissa ilmenevien puutteiden tai väljempien turvanormien vuoksi. Yhdenmukaisten turvallisuussääntöjen avulla olisi myös helpompi varmistaa, että kilpailu ei vääristy sisämarkkinoilla.

- **Suhteellisuusperiaate**

Tässä ehdotuksessa ei ylitetä sitä, mikä on välttämätöntä Euroopan elintärkeiden infrastruktuurien suojaamisen parantamista koskevien tavoitteiden saavuttamista varten. Ehdotuksen keskeiset osat ovat EU:n tason peruskoordinointimekanismin perustaminen, jäsenvaltioiden velvoittaminen määrittämään niiden alueella sijaitsevat elintärkeät infrastruktuurit, näiden infrastruktuurien suojaamiseksi tarvittavien perustavanluonteisten turvatoimenpiteiden toteuttaminen sekä tärkeimpien Euroopan elintärkeiden infrastruktuurien määrittäminen ja nimeäminen. Ehdotuksessa esitetään vähimmäisvaatimukset, jotka on täytettävä, jotta työ elintärkeiden infrastruktuurien suojaamisen parantamiseksi voidaan

aloittaa. Tavoitetta ei voida riittävällä tavalla saavuttaa muiden toimenpiteiden avulla, esimerkiksi antamalla Euroopan elintärkeiden infrastruktuurien suojaamista koskevia ohjeita, koska se ei viime kädessä riittäisi varmistamaan, että suojaamista parannettaisiin kaikkialla EU:n alueella ja että kaikki sidosryhmät voisivat osallistua työhön täysipainoisesti.

- **Sääntelytavan valinta**

Elintärkeiden infrastruktuurien suojaamisesta on huolehdittu eri jäsenvaltioissa eri tavoin niiden erilaisten oikeusjärjestelmien vuoksi. Tämän vuoksi direktiivi on soveltuvin säädöstyyppi, kun halutaan ottaa käyttöön yhteinen menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteinen lähestymistapa niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten.

4) TALOUSARVIOVAIKUTUKSET

Ehdotuksen talousarviovaikutuksia arvioidaan liitteenä olevassa rahoitusselvityksessä.

Direktiivin täytäntöönpanoa edistää osaltaan terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa koskeva erityisohjelma, jonka avulla pyritään parantamaan paitsi väestön suojaamista turvallisuusriskeiltä myös niiden fyysisten voimavarojen, palvelujen ja tietoteknisten laitteiden, verkostojen ja infrastruktuuriomaisuuden suojaamista, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi vakavia seurauksia yhteiskunnan elintärkeille toiminnoille. Vuosina 2007–2013 toteutettava erityisohjelma on osa turvallisuutta ja vapauksien suojelua koskevaa puiteohjelmaa.

Erityisohjelmaa ei sovelleta toimiin, joita rahoitetaan muista välineistä, kuten vakavia hätätilanteita varten perustetusta nopeiden avustustoimien rahoitusvälineestä tai EU:n solidaarisuusrahastosta.

5) LISÄTIEDOT

- **Lainsäädännön kumoaminen**

Mitään voimassa olevia säännöksiä ei tarvitse kumota.

- **Ehdotuksen yksityiskohtainen kuvaus**

1 artiklassa esitetään direktiivin aihe. Direktiivillä otetaan käyttöön yhteinen menettely, jonka avulla voidaan määrittää ja nimetä Euroopan elintärkeät infrastruktuurit eli sellaiset infrastruktuurit, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi seurauksia kahdessa tai useammassa jäsenvaltiossa tai vain yhdessä jäsenvaltiossa siinä tapauksessa, että kyseinen infrastruktuuri sijaitsee toisessa jäsenvaltiossa. Direktiivillä otetaan käyttöön myös yhteinen lähestymistapa arvioida Euroopan elintärkeiden infrastruktuurien suojaamisen parantamistarvetta. Arvioinnin perusteella on helpompi valmistella elintärkeän infrastruktuurin suojaamiseen tarvittavia alakohtaisia erityistoimenpiteitä.

2 artiklassa esitetään direktiivin kannalta keskeiset määritelmät.

3 artiklassa esitetään menettely Euroopan elintärkeiden infrastruktuurien määrittämistä varten. Euroopan elintärkeillä infrastruktuureilla tarkoitetaan sellaisia infrastruktuureja, joiden

vahingoittuminen tai tuhoutuminen aiheuttaisi vakavia seurauksia kahdessa tai useammassa jäsenvaltiossa tai vain yhdessä jäsenvaltiossa siinä tapauksessa, että kyseinen infrastruktuuri sijaitsee toisessa jäsenvaltiossa. Menettely on kolmivaiheinen. Ensin komissio laatii yhdessä jäsenvaltioiden ja sidosryhmien kanssa Euroopan elintärkeiden infrastruktuurien määrittämistä varten horisontaaliset ja alakohtaiset kriteerit, jotka hyväksytään komiteamenettelyllä. Horisontaaliset kriteerit laaditaan sen perusteella, miten vakavaa vahinkoa elintärkeän infrastruktuurin vahingoittuminen tai tuhoutuminen aiheuttaisi. Kunkin infrastruktuurin vahingoittumisen tai tuhoutumisen aiheuttamien seurausten vakavuutta olisi mahdollisuuksien mukaan arvioitava seuraavien kriteerien perusteella:

- vaikutukset väestöön (kohteena olevan väestön määrä);
- taloudelliset vaikutukset (taloudellisten menetysten ja/tai tuotteiden tai palvelujen laadun heikkenemisen suuruusluokka);
- ympäristövaikutukset;
- poliittiset vaikutukset;
- psykologiset vaikutukset;
- kansanterveyteen liittyvät vaikutukset.

Kukin jäsenvaltio määrittää infrastruktuurit, jotka täyttävät em. kriteerit. Lopuksi jäsenvaltiot toimittavat komissiolle tiedot sovitut kriteerit täyttävistä elintärkeistä infrastruktuureistaan. Toimia toteutetaan elintärkeiden infrastruktuurien suojaamiseen liittyvillä painopistealoilla, jotka komissio valitsee liitteessä I olevasta luettelosta vuosittain. Liitteessä I olevaa luetteloa aloista, joilla olisi toteutettava toimia elintärkeiden infrastruktuurien suojaamiseksi, voidaan muuttaa komiteamenettelyllä, kunhan muutokset eivät laajenna direktiivin soveltamisalaa. Tämä tarkoittaa erityisesti sitä, että luetteloa voidaan muuttaa sen sisällön täsmentämiseksi. Komissio katsoo, että kiireellisiä toimia vaativia painopistealoja ovat liikenne ja energia.

4 artiklassa esitetään menettely Euroopan elintärkeiden infrastruktuurien nimeämistä varten. Sen jälkeen kun 3 artiklassa tarkoitettu määrittämismenettely on saatu päätökseen, komissio laatii alustavan luettelon Euroopan elintärkeistä infrastruktuureista. Alustava luettelo perustuu jäsenvaltioiden ilmoituksiin ja muihin komission saamiin tietoihin. Tämän jälkeen luettelo vahvistetaan komiteamenettelyllä.

5 artiklassa säädetään turvallisuussuunnitelmista. Kaikkien Euroopan elintärkeiden infrastruktuurien omistajien/ylläpitäjien on laadittava turvallisuussuunnitelma, jossa määritetään kyseisen infrastruktuurin omistajan ja ylläpitäjän omaisuuserät ja niiden suojaamiseksi tarvittavat turvallisuusratkaisut. Liitteessä II esitetään, että tällaisen turvallisuussuunnitelman tulisi sisältää vähintään seuraavat seikat:

- tärkeiden omaisuuserien määritys;
- riskianalyysi, joka perustuu suurimpiin uhkakuviin, kunkin omaisuuserän haavoittuvuuteen ja siitä mahdollisesti aiheutuviin seurauksiin;
- vastatoimien ja -menettelyjen määrittely, niiden valinta ja tärkeysjärjestys siten, että erotetaan toisistaan:

- **Pysyvät turvatoimet** eli välttämättömät turvallisuusinvestoinnit ja turvakeinot, joita omistaja/ylläpitäjä ei pysty toteuttamaan lyhyellä varoitusajalla. Näitä ovat mm. tiedot yleisistä toimenpiteistä, tekniset toimenpiteet (havaitsemiseen, kulunvalvontaan, suojaamiseen ja ehkäisemiseen tarvittavat järjestelmät), organisatoriset toimenpiteet (hälytys- ja kriisinhallintamenettelyt), valvonta- ja varmennustoimenpiteet, viestintä, tiedottaminen ja koulutus sekä tietojärjestelmien turvallisuus.

- **Porrastetut turvatoimet**, jotka otetaan käyttöön riskien ja uhkien tason perusteella.

Kullakin elintärkeiden infrastruktuurien suojaamisen alalla voidaan laatia alakohtainen turvallisuussuunnitelma liitteessä II esitettyjen vähimmäisvaatimusten pohjalta. Alakohtaiset turvallisuussuunnitelmat voidaan hyväksyä komiteamenettelyllä.

Jos jollakin alalla on jo käytössä vastaavia velvoitteita, voidaan 5 artiklan 2 kohdan mukaisesti myöntää vapautus turvallisuussuunnitelman laatimisesta. Vapautuksen myöntämisestä päätetään komiteamenettelyllä. Esimerkiksi satamien turvallisuuden parantamisesta 26 päivänä lokakuuta 2005 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2005/65/EY asetetut vaatimukset vastaavat turvallisuussuunnitelman laatimista koskevia vaatimuksia.

Kun turvallisuussuunnitelma on laadittu, jokaisen Euroopan elintärkeän infrastruktuurin omistajan/ylläpitäjän on esitettävä se jäsenvaltion toimivaltaiselle viranomaiselle. Kunkin jäsenvaltion on luotava turvallisuussuunnitelmien valvontajärjestelmä sen varmistamiseksi, että elintärkeiden infrastruktuurien omistajat/ylläpitäjät saavat asianmukaista palautetta turvallisuussuunnitelmansa laadusta ja erityisesti riskien ja uhkien arvioinnin riittävyydestä.

6 artiklassa säädetään turvallisuusyhteyshenkilöstä. Artiklan mukaan kaikkien Euroopan elintärkeiden infrastruktuurien omistajien/ylläpitäjien on nimettävä turvallisuusyhteyshenkilö. Yhteyshenkilö vastaa turvallisuuskysymyksiin liittyvästä yhteydenpidosta kyseisen Euroopan elintärkeän infrastruktuurin ja niiden suojaamisesta vastaavien jäsenvaltioiden viranomaisten välillä. Hänen tehtävänään on ottaa vastaan elintärkeiden infrastruktuurien suojaamiseen liittyviä tietoja jäsenvaltion viranomaisilta ja vastaavasti toimittaa viranomaisille tällaisia tietoja kyseisen elintärkeän infrastruktuurin osalta.

7 artiklassa säädetään kertomusten laatimisesta. Artiklan mukaan kertomuksia on laadittava eri vaiheissa. Jokaisen jäsenvaltion on arvioitava Euroopan elintärkeisiin infrastruktuureihin liittyvät riskit ja uhkatekijät. Näiden tietojen pohjalta jäsenvaltiot vaihtavat elintärkeiden infrastruktuurien omistajien/ylläpitäjien kanssa tietoja turvallisuuskysymyksistä (valvonnasta) 5 artiklassa tarkoitetulla tavalla. Koska elintärkeiden infrastruktuurien omistajien/ylläpitäjien on 5 artiklan nojalla laadittava turvallisuussuunnitelma ja esitettävä se jäsenvaltion viranomaisille, jäsenvaltiot velvoitetaan laatimaan yleiskatsaus kullakin elintärkeiden infrastruktuurien suojaamisen alalla ilmenevistä tyypillisistä heikkouksista, uhkatekijöistä ja riskeistä ja toimittamaan nämä tiedot komissiolle. Komissio puolestaan laatii tietojen perusteella arvion siitä, tarvitaanko lisää suojaamistoimenpiteitä. Näiden tietojen pohjalta voidaan myös laatia vaikutustenarviointeja, jotka voidaan liittää tätä alaa koskeviin, myöhemmin esitettäviin ehdotuksiin.

Tässä artiklassa säädetään myös yhteisten menettelyjen laatimisesta Euroopan elintärkeisiin infrastruktuureihin liittyvien riskien, uhkien ja heikkouksien arviointia varten. Tällaiset yhteiset menettelyt hyväksytään komiteamenettelyllä.

8 artiklassa säädetään komission tuesta Euroopan elintärkeille infrastruktuureille. Komissio tukee Euroopan elintärkeiden infrastruktuurien omistajia/ylläpitäjiä huolehtimalla siitä, että niillä on mahdollisuus hyödyntää elintärkeiden infrastruktuurien suojaamiseen liittyviä parhaita käytänteitä ja menettelyjä. Komissio ryhtyy keräämään tällaisia tietoja eri lähteistä, mm. jäsenvaltioilta, ja pyrkii tuottamaan niitä myös itse, minkä jälkeen se asettaa ne asianomaisten tahojen käyttöön.

9 artiklassa säädetään yhteyspisteistä. Jokaisen jäsenvaltion on nimettävä yhteyspiste, jonka tehtävänä on huolehtia elintärkeiden infrastruktuurien suojaamiseen liittyvästä yhteistyöstä ja koordinoinnista. Yhteyspiste vastaa elintärkeiden infrastruktuurien suojaamiseen liittyvien kysymysten koordinoinnista sekä jäsenvaltion sisällä että muiden jäsenvaltioiden ja komission kanssa.

10 artiklassa säädetään elintärkeiden infrastruktuurien suojaamista koskevasta tietojenvaihdosta ja luottamuksellisuudesta. Elintärkeiden infrastruktuurien suojaamiseen liittyvien tietojen luottamuksellisuus ja tietojen vaihto ovat toiminnan keskeisiä osa-alueita, jotka edellyttävät erityistä varovaisuutta. Tämän vuoksi direktiivissä vaaditaan komissiota ja jäsenvaltioita toteuttamaan tarvittavat toimenpiteet tietojen suojaamiseksi. Jäsenvaltioiden viranomaisten on laadittava jokaisesta elintärkeiden infrastruktuurien suojaamiseen liittyviä tietoja käsittelevästä henkilöstä asianmukainen turvallisuusselvitys.

11 artiklassa säädetään komiteamenettelystä. Eräät direktiivin säännökset pannaan täytäntöön komiteamenettelyllä. Komitea muodostuu elintärkeiden infrastruktuurien suojaamisen yhteyspisteistä. Neuvoa-antavaa menettelyä sovelletaan 5 artiklan 2 kohdassa säädettyä tarkoitusta varten eli vapautuksen myöntämiseen turvallisuussuunnitelman laatimista koskevasta velvoitteesta.

Sääntelymenettelyä taas käytetään seuraavissa kysymyksissä:

- 3 artiklan 1 kohta – horisontaalisten ja alakohtaisten kriteerien hyväksyminen Euroopan elintärkeiden infrastruktuurien määrittämistä varten
- 3 artiklan 2 kohta – liitteessä I olevan, elintärkeiden infrastruktuurien suojaamista edellyttävien toimialojen luettelon muuttaminen
- 4 artiklan 2 kohta – Euroopan elintärkeitä infrastruktuureja koskevan alustavan luettelon hyväksyminen
- 5 artiklan 2 kohta – turvallisuussuunnitelmia koskevien alakohtaisten erityisvaatimusten laatiminen
- 7 artiklan 2 kohta – yhteisen mallin laatiminen riskejä, uhkia ja heikkouksia koskevien yleisten kertomusten laatimista varten
- 7 artiklan 4 kohta – yhteisten menetelmien laatiminen riskejä, uhkia ja heikkouksia koskevien arviointien laatimista varten.

2006/0276 (CNS)

Ehdotus:

NEUVOSTON DIREKTIIVI

Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 308 artiklan,

ottaa huomioon Euroopan atomienergiayhteisön perustamissopimuksen ja erityisesti sen 203 artiklan,

ottaa huomioon komission ehdotuksen[1],

ottaa huomioon Euroopan parlamentin lausunnon[2],

ottaa huomioon Euroopan keskuspankin lausunnon[3],

sekä katsoo seuraavaa:

(1) Kesäkuussa 2004 kokoontunut Eurooppa-neuvosto pyysi komissiota laatimaan elintärkeiden infrastruktuurien suojaamista koskevan kokonaisstrategian[4]. Komissio hyväksyi tämän vuoksi 20 päivänä lokakuuta 2004 tiedonannon ”Kriittisen infrastruktuurin suojelu terrorismin torjunnassa”[5]. Siinä esitetään ehdotuksia siitä, miten Euroopassa voitaisiin entistä paremmin ehkäistä elintärkeisiin infrastruktuureihin kohdistuvia terrori-iskuja sekä varautua ja reagoida niihin.

(2) Marraskuun 17 päivänä 2005 komissio hyväksyi vihreän kirjan Euroopan elintärkeiden infrastruktuurien suojaamisohjelmasta[6]. Siinä esitetään eri vaihtoehtoja suojaamisohjelman ja elintärkeiden infrastruktuurien varoitusjärjestelmän (Critical Infrastructure Warning Information Network, CIWIN) toteuttamista varten. Vihreän kirjan perusteella saadusta palautteesta käy selkeästi ilmi, että elintärkeiden infrastruktuurien suojaamista varten on tarpeen perustaa yhteisön kehys. Kommenttien

---

1 EUVL C […], […], s. […].
2 EUVL C […], […], s. […].
3 EUVL C […], […], s. […].
4 Neuvoston asiakirja N:o 10679/2/04 REV 2.
5 KOM(2004) 702.
6 KOM(2005) 576.

mukaan on syytä parantaa elintärkeiden infrastruktuurien suojaamisvalmiutta Euroopassa ja vähentää niiden haavoittuvuutta. Lisäksi kommenteissa korostetaan toissijaisuusperiaatteen noudattamisen ja sidosryhmien kanssa käytävän vuoropuhelun merkitystä.

(3) Joulukuussa 2005 kokoontunut oikeus- ja sisäasioiden neuvosto kehotti komissiota laatimaan ehdotuksen elintärkeiden infrastruktuurien suojaamista koskevaksi EU:n ohjelmaksi. Neuvosto päätti, että vaikka ohjelman avulla olisi pyrittävä suojautumaan kaikkia uhkatekijöitä vastaan, ensisijaisena uhkatekijänä pidettäisiin kuitenkin terrorismia. Tämän lähtökohdan mukaan elintärkeiden infrastruktuurien suojaamisessa tulisi ottaa huomioon sekä ihmisen aiheuttamat että teknologiset uhkatekijät ja luonnononnettomuudet, mutta terrorismia tulisi pitää ensisijaisena uhkatekijänä. Jos jotakin erityisen suurta uhkaa koskevien suojaamistoimien katsotaan olevan jollakin elintärkeiden infrastruktuurien alalla riittävällä tasolla, sidosryhmien olisi keskityttävä torjumaan muita uhkatekijöitä, jotka voivat edelleen vahingoittaa kyseistä infrastruktuuria.

(4) Ensisijainen vastuu elintärkeiden infrastruktuurien suojaamisesta kuuluu nykyään jäsenvaltioille ja elintärkeiden infrastruktuurien omistajille/ylläpitäjille. Tätä tilannetta ei pitäisi muuttaa.

(5) Yhteisössä on tiettyjä elintärkeitä infrastruktuureja, joiden vahingoittuminen tai tuhoutuminen vaikuttaisi kahteen tai useampaan jäsenvaltioon tai johonkin toiseen jäsenvaltioon kuin siihen, jossa kyseinen infrastruktuuri sijaitsee. Tähän saattaa liittyä valtioiden rajat ylittäviä seurauksia, jotka johtuvat toisiinsa liitettyjen, eri alojen infrastruktuurien keskinäisestä riippuvuudesta. Tällaiset Euroopan elintärkeät infrastruktuurit olisi määritettävä ja nimettävä yhteisellä menettelyllä. Myös tarvetta parantaa tällaisten elintärkeiden infrastruktuurien suojaamista olisi arvioitava yhteiseltä pohjalta. Elintärkeiden infrastruktuurien suojaamista koskevat jäsenvaltioiden kahdenväliset yhteistyöjärjestelyt ovat vakiintunut ja tehokas keino vaikuttaa valtioiden rajat ylittäviin elintärkeisiin infrastruktuureihin. Elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman tulisi perustua tällaiseen yhteistyöhön.

(6) Eri toimialoilla on kertynyt erityistä kokemusta ja asiantuntemusta elintärkeiden infrastruktuurien suojaamisesta, ja ne asettavat myös omat vaatimuksensa tälle toiminnalle. Siksi elintärkeiden infrastruktuurien suojaamista koskevan yhteisön menettelyn suunnittelussa ja toteutuksessa olisi otettava huomioon eri alojen erityisominaisuudet. Menettelyn tulisi perustua EU:n tasolla sekä kansallisella ja alueellisella tasolla jo toteutettaviin eri alojen toimenpiteisiin, ja tarvittaessa myös elintärkeiden infrastruktuurien omistajien/ylläpitäjien välillä jo tehtyihin valtioiden rajat ylittäviin keskinäisiin avustussopimuksiin. Koska yksityisellä sektorilla on erittäin merkittävä vastuu riskien valvonnasta ja hallinnasta, liiketoiminnan jatkuvuussuunnittelusta ja katastrofin jälkeisistä elpymistoimista, yhteisön menettelyjen on kannustettava yksityistä sektoria osallistumaan toimintaan täysipainoisesti. Elintärkeistä infrastruktuurialoista on laadittava yhteinen luettelo, koska näin voidaan helpottaa elintärkeiden infrastruktuurien suojaamista koskevan alakohtaisen toimintamallin toteuttamista.

(7) Jokaisen Euroopan elintärkeän infrastruktuurin omistajan/ylläpitäjän olisi laadittava turvallisuussuunnitelma, jossa määritetään elintärkeät omaisuuserät ja esitetään niiden

suojaamiseksi tarvittavat turvallisuusratkaisut. Turvallisuussuunnitelmassa olisi otettava huomioon infrastruktuurin haavoittuvuus, uhkien ja riskien arviointi sekä muut jäsenvaltioiden viranomaisten toimittamat asiaa koskevat tiedot.

(8) Jokaisen Euroopan elintärkeän infrastruktuurin omistajan/ylläpitäjän olisi nimettävä turvallisuusyhteyshenkilö, jotta voidaan helpottaa yhteistyötä ja tietojenvaihtoa elintärkeiden infrastruktuurien suojaamisesta vastaavien kansallisten viranomaisten kanssa.

(9) Eri aloilla ilmenevien riskien, uhkatekijöiden ja heikkouksien tehokas määrittäminen edellyttää tietojenvaihtoa sekä Euroopan elintärkeiden infrastruktuurien omistajien/ylläpitäjien ja jäsenvaltioiden että jäsenvaltioiden ja komission välillä. Kunkin jäsenvaltion olisi kerättävä tietoja alueellaan sijaitsevista Euroopan elintärkeistä infrastruktuureista. Komission olisi saatava jäsenvaltioilta yleistä tietoa heikkouksista, uhkatekijöistä ja riskeistä sekä tarvittaessa mahdollisista turvallisuusvajeista ja eri toimialojen keskinäisistä riippuvuussuhteista. Näiden tietojen pohjalta olisi tarvittaessa laadittava yksityiskohtaisia ehdotuksia Euroopan elintärkeiden infrastruktuurien suojaamisen parantamiseksi.

(10) Jotta voitaisiin helpottaa Euroopan elintärkeiden infrastruktuurien suojaamisen parantamista, olisi kehitettävä yhteisiä menetelmiä infrastruktuuriomaisuuteen liittyvien heikkouksien, uhkatekijöiden ja riskien määrittämistä ja luokittelua varten.

(11) Euroopan elintärkeiden infrastruktuurien suojaamistoimenpiteiden johdonmukainen toteuttaminen ja kaikkien sidosryhmien vastuualueiden selkeä määritteleminen edellyttävät yhteistä toimintakehystä. Euroopan elintärkeiden infrastruktuurien omistajilla/ylläpitäjillä tulisi olla mahdollisuus tutustua elintärkeiden infrastruktuurien suojaamista koskeviin parhaisiin käytänteisiin ja menetelmiin.

(12) Elintärkeiden infrastruktuurien tehokas suojaaminen edellyttää tietojenvaihtoa, koordinointia ja yhteistyötä sekä kansallisella että yhteisön tasolla. Tämä tavoite voidaan saavuttaa parhaiten nimeämällä kussakin jäsenvaltiossa elintärkeiden infrastruktuurien suojaamisen yhteyspiste, joka koordinoi tähän liittyviä kysymyksiä kansallisella tasolla sekä muiden jäsenvaltioiden ja komission kanssa.

(13) Jotta elintärkeiden infrastruktuurien suojaamiseen liittyviä toimia voidaan suunnitella luottamuksellisuutta edellyttävillä aloilla, olisi varmistettava, että tietoja voidaan vaihtaa tämän direktiivin puitteissa johdonmukaisesti ja turvallisesti. Tietyt elintärkeiden infrastruktuurien suojaamiseen liittyvät tiedot ovat luonteeltaan sellaisia, että niiden julkistaminen veisi pohjan yleiseen turvallisuuteen liittyvän yleisen edun suojaamiselta. Koska yksityiskohtaisia tietoja jostakin elintärkeän infrastruktuurin omaisuuserästä voidaan käyttää hyväksi sellaisten toimien suunnittelussa ja toteuttamisessa, joiden tarkoituksena on aiheuttaa infrastruktuurijärjestelmien toiminnalle kestämättömiä seurauksia, tällaiset tiedot olisi luokiteltava salaisiksi, niin että tietoihin voisivat tutustua sekä yhteisön että jäsenvaltioiden tasolla ainoastaan ne, jotka niitä todella tarvitsevat.

(14) Elintärkeitä infrastruktuureja koskevan tietojenvaihdon tulisi tapahtua luottamuksellisesti ja suojatussa ympäristössä. Tietojen jakaminen edellyttää luottamuksellisia suhteita, jotta yritykset ja organisaatiot voivat olla varmoja siitä, että niiden arkaluonteiset tiedot suojataan riittävän hyvin. Teollisuuden toimijoita tulisi

kannustaa jakamaan elintärkeitä infrastruktuureja koskevia tietoja korostamalla, että tietojenvaihdosta koituva hyöty on teollisuuden ja koko yhteiskunnan kannalta tärkeämpää kuin siitä aiheutuvat kustannukset. Elintärkeiden infrastruktuurien suojaamiseen liittyvää tietojenvaihtoa olisi näin ollen pyrittävä edistämään.

(15) Tällä direktiivillä täydennetään yhteisössä ja jäsenvaltioissa voimassa olevia alakohtaisia toimenpiteitä. Jos käytössä on jo yhteisön mekanismeja, niiden käyttöä olisi jatkettava, sillä ne edistävät osaltaan tämän direktiivin täytäntöönpanoa.

(16) Tämän direktiivin täytäntöönpanemiseksi tarvittavista toimenpiteistä olisi päätettävä menettelystä komissiolle siirrettyä täytäntöönpanovaltaa käytettäessä 28 päivänä kesäkuuta 1999 tehdyn neuvoston päätöksen 1999/468/EY[7] mukaisesti.

(17) Tämän direktiivin tavoitteita, eli menettelyn laatimista Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteisen lähestymistavan määrittelyä tällaisten infrastruktuurien suojaamisen parantamistarpeiden arviointia varten, ei voida riittävällä tavalla saavuttaa jäsenvaltioiden toimin, vaan ne voidaan toiminnan laajuuden vuoksi saavuttaa paremmin yhteisön tasolla, joten yhteisö voi toteuttaa toimenpiteitä perustamissopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi.

(18) Tässä direktiivissä kunnioitetaan perusoikeuksia ja noudatetaan erityisesti Euroopan unionin perusoikeuskirjassa tunnustettuja periaatteita,

ON ANTANUT TÄMÄN DIREKTIIVIN:

1 artikla
Kohde

Tällä direktiivillä otetaan käyttöön menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteinen lähestymistapa niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten.

2 artikla
Määritelmät

Tässä direktiivissä tarkoitetaan

a) ’elintärkeällä infrastruktuurilla’ sellaisia omaisuuseriä tai niiden osia, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi ja joihin kuuluvat muun muassa toimitusketju, terveydenhuolto, turvallisuus, turvatoimet sekä väestön taloudellinen ja sosiaalinen hyvinvointi;

b) ’Euroopan elintärkeällä infrastruktuurilla’ sellaisia elintärkeitä infrastruktuureja, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi huomattavia seurauksia

[7] EYVL 184, 17.7.1999, s. 23.

kahdessa tai useammassa jäsenvaltiossa tai vain yhdessä jäsenvaltiossa siinä tapauksessa, että kyseinen infrastruktuuri sijaitsee toisessa jäsenvaltiossa. Tällaiset seuraukset voivat johtua myös siitä, että toimialat ovat riippuvaisia muiden toimialojen infrastruktuureista;

c) ’vakavuudella’ tietyn infrastruktuurin vahingoittumisen tai tuhoutumisen seurauksia, joilla voi olla

- vaikutuksia väestöön (kohteena olevan väestön määrä);
- taloudellisia vaikutuksia (taloudellisten menetysten ja/tai tuotteiden tai palvelujen laadun heikkenemisen suuruusluokka);
- ympäristövaikutuksia;
- poliittisia vaikutuksia;
- psykologisia vaikutuksia;
- kansanterveyteen liittyviä vaikutuksia;

d) ’haavoittuvuudella’ elintärkeän infrastruktuurin suunnittelun, toteutuksen tai toiminnan osan ominaisuutta, joka tekee siitä alttiin jonkin uhkatekijän aiheuttamalle vahingoittumiselle tai tuhoutumiselle; tällä tarkoitetaan myös riippuvuutta muuntyyppisistä infrastruktuureista;

e) ’uhkalla’ mitä tahansa syytä, tilannetta tai tapahtumaa, joka saattaa vahingoittaa elintärkeää infrastruktuuria tai sen osaa tai tuhota sen;

f) ’riskillä’ menetyksen tai vahingoittumisen mahdollisuutta, joka liittyy infrastruktuuriomaisuuserän arvoon sen omistajan/ylläpitäjän kannalta katsottuna ja vahingoittumisen tai tuhoutumisen vaikutusta omaisuuserään sekä sen mahdollisuuden todennäköisyyttä, että jokin tietty uhkatekijä käyttää hyväkseen tiettyä heikkoutta;

g) ’elintärkeän infrastruktuurin suojaamista koskevilla tiedoilla’ elintärkeän infrastruktuurin omaisuuserää koskevia tosiseikkoja, joita voitaisiin niiden tultua julkisiksi käyttää sellaisten toimien suunnittelussa ja toteuttamisessa, joiden tarkoituksena on tuhota elintärkeät infrastruktuurijärjestelmät tai aiheuttaa niiden toiminnalle kestämättömiä seurauksia.

3 artikla
Euroopan elintärkeiden infrastruktuurien määrittäminen

1. Euroopan elintärkeiden infrastruktuurien määrittämisessä tarvittavat horisontaaliset ja alakohtaiset kriteerit hyväksytään 11 artiklan 3 kohdassa tarkoitetulla menettelyllä. Kriteerejä voidaan muuttaa 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

Horisontaaliset kriteerit, joita sovelletaan kaikkiin eri alojen elintärkeisiin infrastruktuureihin, laaditaan tietyn infrastruktuurin vahingoittumisen tai

tuhoutumisen seurausten vakavuuden perusteella. Kriteerit hyväksytään viimeistään [*vuoden kuluttua tämän direktiivin voimaantulosta*].

Painopistealoja varten laaditaan alakohtaiset kriteerit eri alojen elintärkeiden infrastruktuurien ominaispiirteiden ja tarvittaessa sidosryhmien kuulemisen perusteella. Alakohtaiset kriteerit hyväksytään erikseen kutakin painopistealaa varten viimeistään vuoden kuluttua siitä kun kyseinen ala on nimetty painopistealaksi.

2. Komissio valitsee liitteessä I olevan luettelon perusteella kerran vuodessa painopistealat, joita varten 1 kohdassa tarkoitetut alakohtaiset kriteerit laaditaan.

Liitettä I voidaan muuttaa 11 artiklan 3 kohdassa tarkoitetulla menettelyllä, kunhan tämä ei laajenna tämän direktiivin soveltamisalaa.

3. Kunkin jäsenvaltion on määritettävä sellaiset joko sen alueella tai sen ulkopuolella sijaitsevat elintärkeät infrastruktuurit, jotka voivat aiheuttaa seurauksia sen alueella ja jotka täyttävät 1 ja 2 kohdassa säädetyt kriteerit.

Kunkin jäsenvaltion on toimitettava komissiolle tiedot tällä tavoin määritetyistä elintärkeistä infrastruktuureista viimeistään vuoden kuluttua määrittämisessä käytettävien kriteerien hyväksymisestä ja sen jälkeen jatkuvasti.

4 artikla
Euroopan elintärkeiden infrastruktuurien nimeäminen

1. Komissio laatii ehdotuksen Euroopan elintärkeitä infrastruktuureja koskevaksi luetteloksi 3 artiklan 3 kohdan toisen alakohdan nojalla saamiensa ilmoitusten ja muiden käytettävissään olevien tietojen perusteella.

2. Luettelo Euroopan elintärkeistä infrastruktuureista hyväksytään 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

Luetteloa voidaan muuttaa 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

5 artikla
Turvallisuussuunnitelmat

1. Kunkin jäsenvaltion on edellytettävä, että jokainen sen alueella sijaitsevan Euroopan elintärkeän infrastruktuurin omistaja/ylläpitäjä laatii turvallisuussuunnitelman ja pitää sen ajan tasalla sekä tarkistaa sen vähintään kahden vuoden välein.

2. Turvallisuussuunnitelmassa on eriteltävä Euroopan elintärkeän infrastruktuurin omaisuuserät ja esitettävä niiden suojaamiseksi tarvittavat turvallisuusratkaisut liitteen II mukaisesti. Turvallisuussuunnitelmaa koskevia alakohtaisia vaatimuksia, joissa otetaan huomioon voimassa olevat yhteisön toimenpiteet, voidaan hyväksyä 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

Komissio voi päättää 11 artiklan 2 kohdassa tarkoitettua menettelyä noudattaen, että turvallisuussuunnitelman laatimista ja päivittämistä koskevan vaatimuksen voi täyttää noudattamalla liitteessä I luetelluilla aloilla sovellettavia toimenpiteitä.

3. Euroopan elintärkeän infrastruktuurin omistajan/ylläpitäjän on esitettävä turvallisuussuunnitelma toimivaltaiselle jäsenvaltion viranomaiselle vuoden kuluessa siitä kun kyseinen infrastruktuuri on nimetty Euroopan elintärkeäksi infrastruktuuriksi.

Kun 2 kohdan nojalla hyväksytään turvallisuussuunnitelmaa koskevia alakohtaisia vaatimuksia, turvallisuussuunnitelma on esitettävä toimivaltaiselle jäsenvaltion viranomaiselle vasta vuoden kuluttua alakohtaisten vaatimusten hyväksymisestä.

4. Kunkin jäsenvaltion on otettava käyttöön järjestelmä, jonka avulla voidaan varmistaa, että turvallisuussuunnitelmia ja niiden täytäntöönpanoa voidaan säännöllisesti valvoa asianmukaisella tavalla 7 artiklan 1 kohdan mukaisesti suoritetun riskien ja uhkatekijöiden arvioinnin perusteella.

5. Noudattamalla satamien turvallisuuden parantamisesta 26 päivänä lokakuuta 2005 annettua Euroopan parlamentin ja neuvoston direktiiviä 2005/65/EY täytetään turvallisuussuunnitelman laatimista koskeva vaatimus.

6 artikla
Turvallisuusyhteyshenkilö

1. Kunkin jäsenvaltion on edellytettävä, että jokainen sen alueella sijaitsevan Euroopan elintärkeän infrastruktuurin omistaja/ylläpitäjä nimeää turvallisuusyhteyshenkilön, joka vastaa turvallisuuskysymyksiin liittyvästä yhteydenpidosta kyseisen infrastruktuurin omistajan/ylläpitäjän ja näiden infrastruktuurien suojaamisesta vastaavien jäsenvaltion viranomaisten välillä. Turvallisuusyhteyshenkilö on nimettävä vuoden kuluessa siitä kun infrastruktuuri on nimetty Euroopan elintärkeäksi infrastruktuuriksi.

2. Kunkin jäsenvaltion on toimitettava havaittuja riskejä ja uhkatekijöitä koskevat tiedot asianomaisen Euroopan elintärkeän infrastruktuurin turvallisuusyhteyshenkilölle.

7 artikla
Kertomukset

1. Kunkin jäsenvaltion on laadittava arvio alueellaan sijaitseviin Euroopan elintärkeisiin infrastruktuureihin kohdistuvista uhkatekijöistä ja riskeistä vuoden kuluessa siitä, kun ne on nimetty Euroopan elintärkeiksi infrastruktuureiksi.

2. Kunkin jäsenvaltion on toimitettava komissiolle tiivistelmä kullakin liitteessä I tarkoitetulla alalla havaituista heikkouksista, uhkatekijöistä ja riskeistä 18 kuukauden kuluessa siitä kun 4 artiklan 2 kohdassa säädetty luettelo on hyväksytty ja sen jälkeen jatkuvasti kahden vuoden välein.

Näitä kertomuksia varten vahvistetaan yhteinen malli 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

3. Komissio arvioi, tarvitaanko Euroopan elintärkeiden infrastruktuurien suojaamiseksi erityisiä alakohtaisia toimenpiteitä.

4. Euroopan elintärkeiden infrastruktuurien heikkouksien sekä niihin kohdistuvien uhkatekijöiden ja riskien arvioimiseksi voidaan laatia yhteisiä alakohtaisia menetelmiä 11 artiklan 3 kohdassa tarkoitetulla menettelyllä.

8 artikla
Komission tuki Euroopan elintärkeille infrastruktuureille

Komissio tukee Euroopan elintärkeiden infrastruktuurien omistajia/ylläpitäjiä antamalla niille mahdollisuuden hyödyntää elintärkeiden infrastruktuurien suojaamiseen liittyviä parhaita käytänteitä ja menetelmiä.

9 artikla
Elintärkeiden infrastruktuurien suojaamisen yhteyspisteet

1. Kunkin jäsenvaltion on nimettävä elintärkeiden infrastruktuurien suojaamisesta vastaava yhteyspiste.

2. Yhteyspiste vastaa elintärkeiden infrastruktuurien suojaamiseen liittyvien kysymysten koordinoinnista jäsenvaltion sisällä sekä muiden jäsenvaltioiden ja komission kanssa.

10 artikla
Elintärkeiden infrastruktuurien suojaamista koskeva tietojenvaihto ja luottamuksellisuus

1. Tätä direktiiviä soveltaessaan komissio toteuttaa komission päätöksen 2001/844/EY, EHTY, Euratom mukaisesti asianmukaiset toimenpiteet varmistaakseen suojan luottamuksellisuutta edellyttäville tiedoille, joihin sillä on oikeus tutustua tai joita jäsenvaltiot sille toimittavat. Jäsenvaltioiden on toteutettava vastaavat toimenpiteet asiaa koskevan kansallisen lainsäädäntönsä mukaisesti. Yhteisön tai yhden tai useamman jäsenvaltion olennaisille eduille mahdollisesti aiheutuvan vahingon vakavuus on otettava asianmukaisella tavalla huomioon.

2. Jäsenvaltioiden on laadittava asianmukainen turvallisuusselvitys jokaisesta henkilöstä, joka käsittelee niiden puolesta luottamuksellisia tietoja tämän direktiivin mukaisesti.

3. Jäsenvaltioiden on varmistettava, että jäsenvaltioille tai komissiolle toimitettuja elintärkeiden infrastruktuurien suojaamista koskevia tietoja ei käytetä mihinkään muuhun tarkoitukseen kuin elintärkeiden infrastruktuurien suojaamiseen.

11 artikla
Komiteamenettely

1. Komissiota avustaa komitea, joka muodostuu kunkin elintärkeän infrastruktuurin yhteyspisteen edustajista.

2. Jos tähän kohtaan viitataan, sovelletaan päätöksen 1999/468/EY 3 ja 7 artiklaa ottaen huomioon mainitun päätöksen 8 artiklan säännökset.

3. Jos tähän kohtaan viitataan, sovelletaan päätöksen 1999/468/EY 5 ja 7 artiklaa ottaen huomioon mainitun päätöksen 8 artiklan säännökset.

Päätöksen 1999/468/EY 5 artiklan 6 kohdassa tarkoitettu määräaika vahvistetaan yhdeksi kuukaudeksi.

4. Komitea vahvistaa työjärjestyksensä.

12 artikla
Täytäntöönpano

1. Jäsenvaltioiden on saatettava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset voimaan viimeistään 31 päivänä joulukuuta 2007. Niiden on viipymättä toimitettava komissiolle kirjallisina nämä säännökset sekä kyseisiä säännöksiä ja tätä direktiiviä koskeva vastaavuustaulukko.

Näissä jäsenvaltioiden antamissa säädöksissä on viitattava tähän direktiiviin tai niihin on liitettävä tällainen viittaus, kun ne virallisesti julkaistaan. Jäsenvaltioiden on säädettävä siitä, miten viittaukset tehdään.

2. Jäsenvaltioiden on toimitettava tässä direktiivissä tarkoitetuista kysymyksistä antamansa keskeiset kansalliset säännökset kirjallisina komissiolle.

13 artikla
Voimaantulo

Tämä direktiivi tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

14 artikla
Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä

Neuvoston puolesta

LIITE I

LUETTELO ELINTÄRKEÄÄN INFRASTRUKTUURIIN KUULUVISTA TOIMIALOISTA

Toimiala		Alatoimiala	
I	Energia	1	Öljyn ja kaasun tuotanto, jalostus, käsittely, varastointi ja jakelu johdoista muodostuvan verkoston avulla
		2	Sähkön tuotanto ja jakelu
II	Ydinvoimateollisuus	3	Ydinpolttoaineen tuotanto ja varastointi/käsittely
III	Tieto- ja viestintätekniikka	4	Tietojärjestelmien ja -verkostojen suojaaminen
		5	Automaattiset mittaus- ja valvontajärjestelmät (SCADA ym.)
		6	Internet
		7	Kiinteän televerkon palvelujen tarjoaminen
		8	Matkaviestinpalvelujen tarjoaminen
		9	Radioviestintä ja navigointi
		10	Satelliittiviestintä
		11	Radio- ja televisiolähetystoiminta
IV	Vesi	12	Juomaveden jakelu
		13	Veden laadun valvonta
		14	Raakavesivarojen mittaaminen ja valvonta
V	Elintarvikkeet	15	Elintarvikkeiden jakelu sekä elintarviketurvallisuus ja -varmuus
VI	Terveydenhuolto	16	Lääketieteellinen ja sairaalahoito
		17	Lääkkeet, seerumit, rokotukset ja lääkevalmisteet
		18	Biolaboratoriot ja biologiset aineet
VII	Rahoituspalvelut	19	Maksujärjestelmät sekä arvopapereiden selvitys- ja toimitusinfrastruktuurit ja -järjestelmät
		20	Säännellyt markkinat
VIII	Liikenne	21	Maantieliikenne
		22	Rautatieliikenne
		23	Lentoliikenne
		24	Sisävesiliikenne
		25	Meriliikenne (sekä pitkät että lyhyet kuljetukset)
IX	Kemianteollisuus	26	Kemiallisten aineiden tuotanto ja varastointi/käsittely
		27	Vaarallisia (kemiallisia) aineita kuljettavat putkistot
X	Avaruus	28	Avaruus
XI	Tutkimuslaitteistot	29	Tutkimuslaitteistot

LIITE II

TURVALLISUUSSUUNNITELMA

Turvallisuussuunnitelmassa on eriteltävä elintärkeän infrastruktuurin omistajan ja ylläpitäjän omaisuuserät ja esitettävä niiden suojaamiseksi tarvittavat turvallisuusratkaisut. Turvallisuussuunnitelmassa on esitettävä ainakin

– luettelo tärkeistä omaisuuseristä;

– riskianalyysi, joka perustuu tärkeimpiin uhkakuviin, kunkin omaisuuserän haavoittuvuuteen ja siitä mahdollisesti aiheutuviin seurauksiin;

– vastatoimien ja -menettelyjen määrittely, niiden valinta ja tärkeysjärjestys siten, että erotetaan toisistaan:

- **Pysyvät turvatoimet** eli välttämättömät turvallisuusinvestoinnit ja turvakeinot, joita omistaja/ylläpitäjä ei pysty toteuttamaan lyhyellä varoitusajalla. Näitä ovat mm. tiedot yleisistä toimenpiteistä, tekniset toimenpiteet (havaitsemiseen, kulunvalvontaan, suojaamiseen ja ehkäisemiseen tarvittavat järjestelmät), organisatoriset toimenpiteet (hälytys- ja kriisinhallintamenettelyt), valvonta- ja varmennustoimenpiteet, viestintä, tiedottaminen ja koulutus sekä tietojärjestelmien turvallisuus.

- **Porrastetut turvatoimet**, jotka otetaan käyttöön riskien ja uhkien tason perusteella.

SÄÄDÖKSEEN LIITTYVÄ RAHOITUSSELVITYS

Toimintalohko(t): Oikeus- ja sisäasiat

Toiminto: Elintärkeiden infrastruktuurien suojaaminen

TOIMENPITEEN NIMI: Neuvoston direktiivi Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta

1. BUDJETTIKOHTA JA -OTSAKE

-

2. NUMEROTIEDOT

2.1. Toimenpiteen kokonaismäärärahat (B-osa): miljoonaa euroa maksusitoumusmäärärahoina

-

2.2. Toimenpiteen soveltamisaika:

Vuodesta 2006 alkaen.

2.3. Monivuotinen kokonaismenoarvio:

(a) Maksusitoumusmäärärahojen/maksumäärärahojen aikataulu (rahoitustuki) (*ks. kohta 6.1.1*)

miljoonaa euroa (*kolmen desimaalin tarkkuudella*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Yht.
Maksusitoumus-määrärahat	-	-	-	-	-	-	-
Maksumäärärahat	-	-	-	-	-	-	-

(b) Tekninen ja hallinnollinen apu ja tukimenot (*ks. kohta 6.1.2*)

Maksusitoumus-määrärahat	-	-	-	-	-	-	-
Maksumäärärahat	-	-	-	-	-	-	-

a+b yhteensä	-	-	-	-	-	-	-
Maksusitoumus-määrärahat	-	-	-	-	-	-	-

Maksumäärärahat	-	-	-	-	-	-	-

(c) Henkilöstö- ja muiden hallintomenojen kokonaisvaikutus rahoitukseen (*vrt. kohdat 7.2 ja 7.3*)

Maksusitoumus-määrärahat / maksumäärärahat	1,280	1,280	1,280	1,280	1,280	1,280	1,280

a+b+c YHTEENSÄ	1,280	1,280	1,280	1,280	1,280	1,280	1,280
Maksusitoumus-määrärahat	1,280	1,280	1,280	1,280	1,280	1,280	1,280
Maksumäärärahat	1,280	1,280	1,280	1,280	1,280	1,280	1,280

2.4. Yhteensopivuus rahoitussuunnitelman ja rahoitusnäkymien kanssa

Direktiivi on yhteensopiva vuosina 2007–2013 toteutettavan erityisohjelman kanssa, joka koskee terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa.

2.5. Vaikutukset tuloihin

Elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta annettavan direktiivin täytäntöönpanoa edistää osaltaan äskettäin hyväksytty terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa koskeva erityisohjelma (137,5 miljoonaa euroa), jonka avulla pyritään parantamaan paitsi väestön suojaamista turvallisuusriskeiltä myös niiden fyysisten voimavarojen, palvelujen ja tietoteknisten laitteiden, verkostojen ja infrastruktuurin omaisuuserien suojaamista, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi vakavia seurauksia yhteiskunnan elintärkeille toiminnoille. Vuosina 2007–2013 toteutettava erityisohjelma on osa turvallisuutta ja vapauksien suojelua koskevaa puiteohjelmaa. Erityisohjelman soveltamisala on rajoitettu, sillä siihen eivät kuulu laitteistoihin ja varusteisiin liittyvät investoinnit. Erityisohjelmaa ei sovelleta toimiin, joita rahoitetaan muista välineistä, kuten vakavia hätätilanteita varten perustetusta nopeiden avustustoimien rahoitusvälineestä.

Terrori-iskujen ja muiden turvallisuusriskien ehkäisemisen ja torjuntavalmiuden osalta erityisohjelman tarkoituksena on

a) kehittää, edistää ja tukea elintärkeisiin infrastruktuureihin liittyvien riskien ja uhkatekijöiden arviointia muun muassa toteuttamalla paikan päällä tehtäviä evaluointeja, jotta voitaisiin tunnistaa uhkatekijät ja heikkoudet ja arvioida tarvetta parantaa infrastruktuurien turvatoimia.

b) edistää ja tukea yhteisiä operatiivisia toimenpiteitä, joiden tarkoituksena on parantaa valtioiden rajat ylittävien toimitusketjujen turvallisuutta, kunhan kilpailu ei vääristy sisämarkkinoilla.

c) edistää ja tukea vähimmäisturvallisuusnormien laatimista, parhaiden käytänteiden vaihtoa, riskinarviointia, eri alojen infrastruktuurien vertailussa ja painopisteiden asettamisessa käytettäviä menetelmiä sekä elintärkeiden

infrastruktuurien suojaamiseen liittyvien heikkouksien ja keskinäisten riippuvuussuhteiden analysoimista.

d) edistää ja tukea elintärkeiden infrastruktuurien suojaamiseen liittyvää yhteisön laajuista koordinointia ja yhteistyötä, tarvittaessa laatimalla ehdotuksia vähimmäissuojatoimenpiteistä ja yhteisistä suuntaviivoista.

Terrori-iskujen ja muiden turvallisuusriskien seurausten hallinnan osalta erityisohjelman tarkoituksena on

a) kehittää, edistää ja tukea taitotiedon, kokemusten ja teknologian vaihtoa.

b) kehittää, edistää ja tukea tarvittavien menetelmien ja valmiussuunnitelmien laatimista.

c) varmistaa, että yleisen kriisinhallinnan, nopeiden hälytysjärjestelmien ja väestönsuojelujärjestelyjen yhteydessä myös turvallisuuskysymyksiä koskeva erityisasiantuntemus on käytettävissä reaaliajassa.

Direktiiviehdotuksella ei näin ollen ole vaikutuksia tuloihin.

3. BUDJETTITIEDOT

Menolaji		**Uusi**	**EFTA osallistuu**	**Ehdokasmaat osallistuvat**	**Rahoitus-näkymien otsake**
Ei-pakoll.	EI-JM	-	-	-	Ei ole

4. OIKEUSPERUSTA

Ehdotuksen oikeusperusta on Euroopan yhteisön perustamissopimuksen 308 artikla.

5. KUVAUS JA PERUSTELUT

5.1. Yhteisön tuen tarve

5.1.1. Tavoitteet

Elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman yhteisen kehyksen luomiseen soveltuu parhaiten direktiivi, koska elintärkeiden infrastruktuurien suojaamisesta on huolehdittu eri jäsenvaltioissa eri tavoin ja koska niiden oikeusperinteet eroavat toisistaan. EU:n tasolla toteutettavan suojaamisohjelman tavoitteet voidaan saavuttaa täysimääräisesti jo käytössä olevien toimien pohjalta esittämällä joitakin keskeisiä ehdotuksia ja antamalla jäsenvaltioille mahdollisuus käyttää menettelyjä, jotka parhaiten soveltuvat niiden tarpeisiin.

5.1.2. Ennakkoarviointiin liittyvät toimenpiteet

Kaikkia elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman kannalta olennaisia sidosryhmiä on kuultu. Tätä varten on toteutettu seuraavat toimet:

- Elintärkeitä infrastruktuureja koskeva vihreä kirja julkaistiin 17. marraskuuta 2005, ja kuulemismenettely päättyi 15. tammikuuta 2006. Kuulemisen yhteydessä esitettyihin kysymyksiin saatiin virallinen vastaus 22 jäsenvaltiolta. Lisäksi vihreään kirjaan saatiin kommentteja noin sadalta yksityisen sektorin toimijalta. Yleensä ottaen vastauksissa kannatetaan elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman perustamista.

- Komissio on järjestänyt kolme seminaaria, joissa on käsitelty elintärkeiden infrastruktuurien suojaamista (kesäkuussa 2005, syyskuussa 2005 ja maaliskuussa 2006). Kaikkiin seminaareihin osallistui edustajia eri jäsenvaltioista. Syyskuussa 2005 ja maaliskuussa 2006 pidettyihin seminaareihin kutsuttiin myös yksityisen sektorin edustajia.

- Elintärkeiden infrastruktuurien suojaamisen yhteyspisteiden epäviralliset tapaamiset. Komissio on järjestänyt jäsenvaltioiden yhteyspisteille kaksi tapaamista (joulukuussa 2005 ja helmikuussa 2006).

- Epäviralliset tapaamiset yksityisen sektorin edustajien kanssa. Useita epävirallisia tapaamisia on järjestetty myös yksittäisten yritysten sekä eri toimialajärjestöjen edustajien kanssa.

- Komission sisällä suojaamisohjelmaa on valmisteltu elintärkeiden infrastruktuurien suojaamista käsittelevän työryhmän säännöllisissä kokouksissa. Työryhmä on EU:n sisäistä terrorismia käsittelevän komission yksiköiden välisen työryhmän alaryhmä.

5.2. Suunnitellut toimet ja yhteisön rahoitustukea koskevat yksityiskohtaiset säännöt

Ehdotuksen talousarviovaikutuksia arvioidaan liitteenä olevassa rahoitusselvityksessä.

5.3. Toteutustapa

Direktiivi ei vaikuta EU:n talousarvioon.

6. RAHOITUSVAIKUTUKSET

6.1. Kokonaisrahoitusvaikutus B-osaan (koko ohjelmakaudeksi)

6.1.1. Rahoitustuki

-

6.1.2. Tekninen ja hallinnollinen apu, tukimenot ja tietotekniikkakustannukset (maksusitoumusmäärärahat)

-

6.2. Toimenpidekohtainen kustannuslaskelma, B-osa (koko ohjelmakaudeksi)

-

7. VAIKUTUKSET HENKILÖSTÖÖN JA HALLINTOMENOIHIN

7.1. Vaikutus henkilöstöön

Laji		Toimen hallinnointiin tarvittava nykyinen henkilöstö		Yht.	Toimintaan liittyvien tehtävien kuvaus
		Vakinaisten virkojen ja/tai toimien määrä	Väliaikaisten toimien määrä		
Virkamiehet tai väliaikaiset toimihenkilöt	A B C	8 A 1 B	1 C	10	Tietojen kerääminen ja käsittely. Komitean kokousten valmistelu.
Muut henkilöresurssit					
Yht.		9	1	10	

Henkilöstö- ja hallintotarpeet katetaan toimenpiteestä vastaavalle pääosastolle myönnetyistä varoista vuotuisen talousarvion puitteissa.

7.2. Henkilöresurssien kokonaisrahoitusvaikutus

Laji	Määrä (euroina)	Laskentamenetelmä*
Virkamiehet Väliaikaiset toimihenkilöt	1 080 000 48 000	108 000x10=1 080 000 4 000 x 12 = 48 000
Muut henkilöresurssit (budjettikohta ilmoitettava)		
Yht.	1 128 000	

Määrät vastaavat 12 kuukauden kokonaismenoja.

7.3. Toiminnasta johtuvat muut hallintomenot

Budjettikohta (numero ja nimi)	Määrä euroina	Laskentamenetelmä
Kokonaismääräraha (osasto A7)		
A0701 – Virkamatkat	24 000	2 000 x 12 kk = 24 000
A07030 – Kokoukset	-	-
A07031 – Pakolliset komiteat	128 000	32 000 x 4 kokousta/vuosi = 128 000
A07032 – Ei-pakolliset komiteat	-	-
A07040 – Konferenssit	-	-
A0705 – Selvitykset ja kuulemiset	-	-
Muut menot (eriteltävä)		

Tietojärjestelmät (A-5001/A-4300)	-	-
Muut menot: A-osa (eriteltävä)		
Yht.	152 000	

Määrät vastaavat 12 kuukauden kokonaismenoja.

Ilmoitetaan, millaisesta komiteasta on kysymys ja mihin ryhmään se kuuluu.

I.	Yhteensä vuodessa (7.2 + 7.3)	1 280 000
II.	Toiminnan kesto	Käynnissä
III.	Toiminnan kokonaiskustannukset (I x II)	

8. SEURANTA JA ARVIOINTI

8.1. Seurantajärjestelmä

-

8.2. Arvioinnin yksityiskohtaiset säännöt ja arviointijaksot

-

9. PETOSTENTORJUNTA

-

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 12.12.2006
KOM(2006) 787 slutlig

2006/0276 (CNS)

Förslag till

RÅDETS DIREKTIV

om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna

(framlagt av kommissionen)

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

MOTIVERING

1) BAKGRUND TILL FÖRSLAGET

- **Motiv och syfte**

Europeiska rådet bad i juni 2004 kommissionen att utarbeta en övergripande strategi för skydd av kritisk infrastruktur. Med anledning av detta antog kommissionen den 20 oktober 2004 meddelandet ”Skydd av kritisk infrastruktur i kampen mot terrorismen” med förslag om vad som skulle kunna förbättra de förebyggande åtgärderna, beredskapen och insatserna i Europa gentemot terrorattacker som drabbar kritisk infrastruktur.

I rådets slutsatser när det gäller att förebygga, ha beredskap för och bemöta terrorattacker samt i EU:s solidaritetsprogram avseende konsekvenserna av terrorhot och terrorattacker, som antogs av rådet i december 2004, godkändes kommissionens avsikt att föreslå ett europeiskt program för skydd av kritisk infrastruktur (EPCIP – dvs. European Programme for Critical Infrastructure Protection), och vidare lämnades samtycke till att kommissionen inrättar ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN – dvs. Critical Infrastructure Warning Information Network).

I november 2005 antog kommissionen en grönbok om ett europeiskt program för skydd av kritisk infrastruktur (EPCIP – dvs. *European Programme for Critical Infrastructure Protection*), där det redogjordes för olika åtgärder som kommissionen kunde vidta för att utforma ett sådant program samt inrätta ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN – dvs. *Critical Infrastructure Warning Information Network*).

I december 2005 uppmanade rådet (rättsliga och inrikes frågor) kommissionen att lägga fram ett förslag till europeiskt program för skydd av kritisk infrastruktur senast i juni 2006.

I föreliggande direktivförslag redovisas de åtgärder för kartläggning och klassificering av europeisk kritisk infrastruktur som kommissionen föreslår, samt en bedömning av behovet av ökat skydd för sådan infrastruktur.

- **Allmän bakgrund**

Det finns ett antal kritiska infrastrukturer inom Europeiska unionen där driftstörningar eller förstörelse skulle drabba två eller flera medlemsstater. Även om kritisk infrastruktur i en enskild medlemsstat drabbas, kan detta också ge effekter i en eller flera andra medlemsstater. Infrastruktur som på så sätt har en gränsöverskridande dimension bör kartläggas och klassificeras som *europeisk kritisk infrastruktur*. Kartläggningen kan bara ske genom ett gemensamt förfarande, i kombination med en bedömning av behovet av att skydda den infrastruktur som kartläggs.

Med tanke på den gränsöverskridande dimensionen skulle en integrerad och EU-övergripande ansats vara ett lämpligt komplement när det gäller att bedöma sårbarhet och brister i de befintliga skyddsåtgärderna, och en sådan ansats skulle samtidigt tillföra ett mervärde till de program för att skydda kritisk infrastruktur som redan inrättats i medlemsstaterna. En sådan integrerad ansats skulle också på ett påtagligt sätt bidra till den inre marknadens fortsatta livaktighet och kapacitet att skapa ökat välstånd.

Eftersom det inom vissa sektorer finns särskilda erfarenheter, sakkunskap och behov med avseende på skyddet av kritisk infrastruktur, bör EU vid utvecklingen och genomförandet av en gemensam strategi för skydd av sådan infrastruktur beakta särdragen inom olika sektorer och utgå från de åtgärder som redan vidtagits på sektornivå. Man behöver sammanställa en gemensam förteckning över sektorer där det finns kritisk infrastruktur för att underlätta genomförandet av en sektorsvis strategi för skyddet av kritisk infrastruktur.

- **Behovet av en gemensam ram**

Det krävs en gemensam ram för att samordnade och enhetliga insatser för att förbättra skyddet av europeisk kritisk infrastruktur skall kunna genomföras. Detta är också nödvändigt för att kunna avgränsa de olika parternas ansvar på ett tydligt sätt. Ett system med frivilliga åtgärder skulle visserligen ge god flexibilitet, men inte den stabila grund som krävs, och det skulle inte heller bli tillräckligt klart vem som ansvarar för vad, eller vilka rättigheter och skyldigheter de olika parterna har.

Ett förfarande för att kartlägga och klassificera europeisk kritisk infrastruktur och en gemensam strategi för att bedöma behovet av förbättrat skydd för sådan infrastruktur kan endast utarbetas genom ett direktiv för att på så sätt garantera

- en adekvat skyddsnivå för europeisk kritisk infrastruktur,
- att alla berörda parter har samma rättigheter och skyldigheter, och
- att den inre marknadens stabilitet bibehålls.

En skada på eller förlust av en del av infrastrukturen i en medlemsstat kan få negativa återverkningar på såväl flera andra medlemsstater som på den europeiska ekonomin som helhet. Detta blir alltmer sannolikt i takt med att den nya tekniken (t.ex. Internet) och avregleringen av marknaderna (t.ex. el- och gasleveranser) medför att stora delar av infrastrukturen blir en del i ett större nät. I en sådan situation är skyddsåtgärderna inte effektivare än sin svagaste länk. Detta innebär att en gemensam skyddsnivå kan vara nödvändig.

- **En dialog med berörda parter inom olika sektorer**

För att ett skydd skall vara effektivt krävs kommunikation, samordning, och samarbete mellan alla berörda parter nationellt och på EU-nivå.

Det är viktigt att även den privata sektorn engageras i arbetet, eftersom kritisk infrastruktur ofta är i privat ägo. Varje operatör måste kunna ansvara för sin egen riskhantering, och det är normalt operatörens eget beslut vilka skyddsåtgärder och vilken avbrottsplanering (reservdrift, åtgärder vid driftsstopp) man vill införa. Avbrottsplaneringen bör utformas enligt normala drifts- och affärshänsyn, och lösningarna bör i möjligaste mån bygga på gängse affärsmässiga grunder.

Det finns som regel särskilda erfarenheter, behov och sakkunskaper när det gäller skydd av kritisk infrastruktur i varje sektor.

I linje med remissvaren på grönboken om ett europeiskt program för skydd av kritisk infrastruktur bör EU således till fullo involvera den privata sektorn i arbetet, ta hänsyn till

särdragen i olika sektorer och bygga vidare på de sektorsspecifika skyddsåtgärder som redan införts.

- **Gällande bestämmelser**

Det finns för närvarande inga EU-övergripande bestämmelser om skydd av kritisk infrastruktur. Genom detta direktiv fastställs därför ett förfarande för att kartlägga och klassificera europeisk kritisk infrastruktur och en gemensam metod för att bedöma behovet av ett stärkt skydd för sådan infrastruktur.

Det finns redan relevanta sektorsbestämmelser inom många områden:

- Informationsteknik:

  (a) ”Direktivet om samhällsomfattande tjänster”, 2002/22/EG, behandlar bland annat frågan om de allmänna kommunikationsnätens integritet.

  (b) ”Auktorisationsdirektivet”, 2002/20/EG, behandlar bland annat frågan om de allmänna kommunikationsnätens integritet.

  (c) Direktiv 2002/58/EG behandlar bland annat frågan om säkerhet i elektroniska kommunikationsnät.

  (d) Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem.

  (e) Förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet (ENISA).

- Vård och läkemedel:

  (a) Europaparlamentets och rådets beslut nr 2119/98/EG av den 24 september 1998 om att bilda ett nätverk för epidemiologisk övervakning och kontroll av smittsamma sjukdomar i gemenskapen.

  (b) Kommissionens direktiv 2003/94/EG av den 8 oktober 2003 om fastställande av principer och riktlinjer för god tillverkningssed i fråga om humanläkemedel och prövningsläkemedel för humant bruk.

- Bank och finans:

  (a) Europaparlamentets och rådets direktiv 2004/39/EG av den 21 april 2004 om marknader för finansiella instrument (”MiFID-direktivet”).

  (b) Standarder för detaljistbetalningar i euro, antagna av Europeiska centralbankens styrelse i juni 2003.

  (c) Europaparlamentets och rådets direktiv 2006/48/EG av den 14 juni 2006 om rätten att starta och driva verksamhet i kreditinstitut.

  (d) Europaparlamentets och rådets direktiv 2006/49/EG av den 14 juni 2006 om kapitalkrav för värdepappersföretag och kreditinstitut.

(e) Förslag till Europaparlamentets och rådets direktiv om betaltjänster på den inre marknaden och om ändring av direktiven 97/7/EG, 2002/12/EG och 2002/65/EG (KOM(2005) 603).

(f) Europaparlamentets och rådets direktiv 2000/46/EG av den 18 september 2000 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet.

(g) Europaparlamentets och rådets direktiv 1998/26/EG från 19 maj 1998 om slutgiltig avveckling i system för överföring av betalningar och värdepapper.

- Transport:

(a) Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar.

(b) Kommissionens förordning (EG) nr 884/2005 av den 10 juni 2005 om fastställande av förfaranden för utförande av kommissionens inspektioner på området för sjöfartsskydd.

(c) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd.

(d) Europaparlamentets och rådets förordning (EG) nr 2320/2002 av den 16 december 2002 om införande av gemensamma skyddsregler för den civila luftfarten.

(e) Kommissionens förordning (EG) nr 622/2003 av den 4 april 2003 om åtgärder för att genomföra gemensamma grundläggande standarder avseende luftfartsskydd.

(f) Kommissionens förordning (EG) nr 1217/2003 av den 4 juli 2003 om fastställande av gemensamma specifikationer för nationella säkerhets- och kvalitetskontrollprogram för civil luftfart.

(g) Kommissionens förordning (EG) nr 1486/2003 av den 22 augusti 2003 om fastställande av förfaranden för utförande av kommissionens inspektioner på området luftfartsskydd för den civila luftfarten.

(h) Kommissionens förordning (EG) nr 68/2004 av den 15 januari 2004 om ändring av förordning (EG) nr 622/2003 om åtgärder för att genomföra gemensamma grundläggande standarder avseende luftfartsskydd.

(i) Europaparlamentets och rådets förordning nr (EG) nr 849/2004 av den 29 april 2004 om ändring av förordning nr (EG) nr 2320/2002 om införande av gemensamma skyddsregler för den civila luftfarten.

(j) Kommissionens förordning nr (EG) nr 1138/2004 av den 21 juni 2004 om en gemensam definition av känsliga delar av behörighetsområden på flygplatser.

(k) Kommissionens förordning (EG) nr 781/2005 av 24.maj.2005 om ändring av förordning (EG) nr 622/2003 om åtgärder för att genomföra gemensamma grundläggande standarder avseende luftfartsskydd.

(l) Kommissionens förordning (EG) nr 857/2005 av den 6 juni 2005 om ändring av förordning (EG) nr 622/2003 om åtgärder för att genomföra gemensamma grundläggande standarder avseende luftfartsskydd.

(m) Direktiv 2001/14 om tilldelning av infrastrukturkapacitet för järnvägen.

(n) Transport av farligt gods på järnväg omfattas av direktiv 1996/49, ändrat genom direktiv 2004/10 (genom vilket RID 2005 antogs).

(o) Konventionen om fysiskt skydd av kärnämne och kärnanläggningar (ursprungligen undertecknad 1981 och trädde i kraft 1987).

- Kemi:

(a) Frågan om riskverksamheter tas upp i rådets direktiv 96/82/EG av den 9 december 1996 om åtgärder för att förebygga och begränsa följderna av allvarliga olyckshändelser där farliga ämnen ingår (”Seveso II-direktivet”), ändrat genom Europaparlamentets och rådets direktiv 1003/105/EG av den 16 december 2003

- Kärnenergiindustrin:

(a) Rådets direktiv 89/618/Euratom av den 27 november 1989 om information till allmänheten om hälsoskyddsåtgärder och förhållningsregler i händelse av en nödsituation som medför risk för strålning

(b) Rådets beslut 87/600/Euratom av den 14 december 1987 om en gemenskapsordning för ett snabbt informationsutbyte i händelse av en nödsituation som medför risk för strålning.

- **Förenlighet med EU:s politik och mål inom andra områden**

Detta förslag är helt och hållet förenligt med Europeiska unionens mål, och i synnerhet målet ”att bevara och utveckla ett område med frihet, säkerhet och rättvisa, där den fria rörligheten för personer garanteras, samtidigt som lämpliga åtgärder vidtas avseende kontroller vid yttre gränser, asyl, invandring och förebyggande och bekämpande av brottslighet”.

Förslaget är också förenligt med övriga målsättningar, eftersom det inte har till syfte att ersätta befintliga åtgärder till skydd för europeisk kritisk infrastruktur, utan att komplettera dessa åtgärder.

2) SAMRÅD OCH KONSEKVENSBEDÖMNING

- **Samråd med berörda parter**

Under arbetet med att utveckla det europeiska programmet för skydd av kritisk infrastruktur har alla berörda parter rådfrågats:

- Den 17 november 2005 antogs grönboken om programmet, och perioden för samråd kring detta dokument pågick fram till den 15 januari 2006. Under detta samråd lämnades officiella remissvar av 22 medlemsstater. Dessutom yttrade sig ett hundratal representanter för den privata sektorn över grönboken. Sammantaget var svaren tämligen positiva till idén om att inrätta programmet.

- Tre seminarier om skydd av kritisk infrastruktur har hållits i kommissionens regi, i juni och i september 2005 samt i mars 2006. Alla tre seminarierna riktade sig till företrädare för medlemsstaterna, och till de två senare (september 2005 och mars 2006) inbjöds också den privata sektorn.

- Det har hållits informella möten för företrädare för de ”kontaktpunkter” som inrättats för frågor som gäller skydd av kritisk infrastruktur. Kommissionen stod som värd för två sådana möten, som hölls i december 2005 och februari 2006.

- Det har också hållits ett antal informella möten med företrädare för den privata sektorn, bland annat från enskilda företag och från näringslivsorganisationer.

- Inom kommissionen har arbetet med programmet för skydd av kritisk infrastruktur drivits framåt genom regelbundna möten inom den undergrupp för skydd av kritisk infrastruktur som inrättats under den sektorsövergripande arbetsgruppen för interna aspekter på terrorismen (Inter-Service Group on the Internal Aspects of Terrorism).

- **Insamling och tillvaratagande av synpunkter**

Synpunkter från experter har tagits in under ett flertal möten och seminarier under 2004–2006, samt under samrådet om grönboken. Uppgifter har samlats in från samtliga berörda parter.

- **Konsekvensanalys**

Ett exemplar av konsekvensanalysen för det europeiska programmet för skydd av kritisk infrastruktur bifogas detta förslag.

3) RÄTTSLIGA ASPEKTER AV DET FÖRESLAGNA DIREKTIVET

- **Sammanfattning av den föreslagna åtgärden**

Genom den föreslagna åtgärden skapas sektorsövergripande ramar för kartläggning och klassificering av europeisk kritisk infrastruktur samt en bedömning av behovet av ökat skydd för sådan infrastruktur.

- **Rättslig grund**

Den rättsliga grunden för förslaget är artikel 308 i fördraget om upprättandet av Europeiska gemenskapen.

- **Subsidiaritetsprincipen**

Förslaget är förenligt med subsidiaritetsprincipen, eftersom de åtgärder som föreslås inte kan genomföras av en enskild medlemsstat, utan måste vidtas på EU-nivå. Även om det är varje medlemsstats ansvar att skydda den kritiska infrastruktur som omfattas av dess rättssystem, är det av central vikt för EU:s säkerhet att skydda sådan infrastruktur vars funktion påverkar två eller flera medlemsstater, eller sådan infrastruktur i en medlemsstat som är av stor vikt för en annan, så att inte svagheter eller lägre säkerhetsnivå i en medlemsstat drabbar en eller flera andra. Den snedvridning av konkurrensen inom den inre marknaden som kan följa av stora avvikelser mellan säkerhetsbestämmelser i olika medlemsstater skulle också kunna minskas genom att reglerna blir mer likvärdiga.

- **Proportionalitetsprincipen**

Förslaget går inte utöver vad som krävs för att uppnå det grundläggande målet att skydda europeisk kritisk infrastruktur. Huvudelementen i förslaget är att en samordningsmekanism skall inrättas på EU-nivå, vilket bland annat innebär att medlemsstaterna skall bli skyldiga att själva kartlägga sina kritiska infrastrukturer, att en uppsättning grundläggande skyddsbestämmelser för kritisk infrastruktur skall införas samt att de ”europeiska” kritiska infrastrukturerna (dvs. som berör flera medlemsstater) skall kartläggas och klassificeras. I förslaget presenteras därför de krav som minst måste införas för att ett arbete för skydd av kritisk infrastruktur skall kunna inledas. Andra metoder, t.ex. att styra programmets genomförande med hjälp av riktlinjer, ger inte tillräckliga garantier för att skyddsnivån faktiskt kommer att stärkas i hela EU och att alla berörda parter engagerar sig i arbetet.

- **Val av regleringsform**

Medlemsstaterna har olika rättssystem och olika sätt att hantera frågan om kritisk infrastruktur. Kommissionens bedömning är därför att ett direktiv är det bästa sättet att skapa ett gemensamt förfarande för att kartlägga och klassificera europeisk kritisk infrastruktur och en samsyn när det gäller bedömning av behoven av ett stärkt skydd för sådan infrastruktur.

4) BUDGETKONSEKVENSER

En bedömning av förslagets konsekvenser för budgeten redovisas i den bifogade finansieringsöversikten.

Programmet för förebyggande, beredskap och konsekvenshantering i kampen mot terrorism och andra säkerhetsrisker (2007–2013) kommer att bidra till genomförandet av det föreslagna direktivet när det gäller att skydda befolkningen mot risker för den personliga säkerheten och hot riktade mot de fysiska resurser, tjänster, IT-kapacitet, nätverk och infrastrukturer som – om de förstörs eller utsätts för driftsstörningar – allvarligt kan störa grundläggande samhällsfunktioner. Programmet utgör en del av det allmänna programmet ”säkerhet och skydd av friheter”.

Det omfattar inte sådana aspekter som redan täcks av andra finansiella instrument, t.ex. instrumentet för snabb reaktion vid större katastrofer eller Europeiska unionens solidaritetsfond.

5) KOMPLETTERANDE INFORMATION

- **Upphävande av gällande lagstiftning**

Det finns i det här fallet ingen gällande lagstiftning som måste upphävas.

- **Närmare redogörelse för förslaget**

Artikel 1 – Syftet med direktivet presenteras. I direktivet fastställs ett gemensamt förfarande för att kartlägga och klassificera *europeisk kritisk infrastruktur.* Med detta avses infrastruktur där en driftstörning eller förstörelse skulle drabba två eller flera medlemsstater, eller där en annan medlemsstat skulle drabbas om infrastruktur belägen i en annan medlemsstat utsattes för driftstörningar eller förstörelse. Genom direktivet införs också en gemensam metod för att bedöma behoven av ett stärkt skydd av sådan infrastruktur. Bedömningen skall sedan ligga till grund för utarbetandet av särskilda skyddsåtgärder inom vissa sektorer som omfattar kritiska infrastrukturer.

Artikel 2 – Definitioner av de centrala begrepp som används i direktivet.

Artikel 3 – I denna artikel regleras hur europeisk kritisk infrastruktur kartläggs. Med europeisk kritisk infrastruktur avses infrastruktur där en driftstörning eller förstörelse skulle drabba två eller flera medlemsstater, eller där en annan medlemsstat skulle drabbas om infrastruktur belägen i en annan medlemsstat utsattes för driftstörningar eller förstörelse. Förfarandet är indelat i tre steg. I det första steget fastställer kommissionen, medlemsstaterna och berörda parter generella och sektorsspecifika kriterier för vad som skall kartläggas som en europeisk kritisk infrastruktur, och dessa kriterier antas sedan formellt genom ett kommittéförfarande. De generella kriterierna grundas på hur allvarlig en driftstörning i eller förstörelse av en viss kritisk infrastruktur är. Denna bedömning grundas i sin tur (såvitt som möjligt) på följande faktorer:

- Konsekvenser för allmänheten (antal drabbade).
- Ekonomiska konsekvenser (omfattningen av förluster eller försämring av varor eller tjänster osv.).
- Effekter på miljön.
- Politiska effekter.
- Psykologiska effekt.
- Effekter på folkhälsan.

I nästa steg kartlägger varje medlemsstat de infrastrukturer som bedöms uppfylla kriterierna, och i det tredje steget anmäler de dessa uppgifter till kommissionen. Det arbete som måste genomföras sker under ledning av prioriterade sektorsorgan som kommissionen utser på årsbasis bland dem som återfinns i bilaga I. Förteckningen över sektorsorgan i bilaga I kan

ändras genom kommittéförfarandet så länge detta inte vidgar direktivets giltighetsområde. Detta innebär särskilt ändringar i förteckningen som endast får ske för att klargöra innehållet. Kommissionen anser att transport- och energisektorerna skall vara prioriterade områden.

Artikel 4 – I denna artikel lämnas en redogörelse för hur europeiska kritiska infrastrukturer skall klassificeras. När kartläggningen har fullbordats enligt artikel 3 upprättar kommissionen en förteckning över europeiska kritiska infrastrukturer. Denna förteckning grundas på de anmälningar som inkommit från medlemsstaterna samt andra relevanta uppgifter som kommissionen förfogar över. Förteckningen antas genom ett kommittéförfarande.

Artikel 5 – Säkerhetsplan. Enligt artikel 5 måste alla som äger eller driver infrastruktur som klassificerats såsom europeisk kritisk infrastruktur upprätta en säkerhetsplan. Av denna skall framgå exakt vilka anläggningar ägaren eller operatören sköter, samt vilka säkerhetsåtgärder som vidtagits för att skydda dessa. I bilaga II anges minimikrav för vad som skall ingå i en sådan säkerhetsplan, i korthet:

- En förteckning över viktiga anläggningar.

- En riskanalys grundad på de mest väsentliga hotbilderna, en beskrivning av varje tillgångs känslighet samt en redogörelse för potentiella konsekvenser av en skada.

- Kartläggning och urval av motåtgärder och tillvägagångssätt samt prioritering bland dessa. Åtgärderna kan indelas i följande huvudkategorier:

    - **Permanenta säkerhetsåtgärder**, dvs. oumbärliga säkerhetsinvesteringar och resurser som inte kan installeras eller införas av ägare eller operatörer med kort varsel. Denna rubrik skall innehålla uppgifter om allmänna och tekniska åtgärder (bl.a. vilka system som finns installerade för kartläggning av hot, skydd mot fysiskt intrång, skydd av anläggningar samt förebyggande åtgärder), organisatoriska åtgärder (larmrutiner och krishantering), kontroller, kommunikation, utbildning och åtgärder för ökad medvetenhet samt IT-säkerhet.

    - **Graderade säkerhetsåtgärder**, som kan aktiveras i enlighet med varierande hotnivåer.

Varje sektor som omfattar kritisk infrastruktur kan utveckla sektorsspecifika säkerhetsplaner på grundval av minimikraven i bilaga II, som också kan antas genom kommittéförfarande.

Vad gäller de sektorer som redan omfattas av liknande krav kan det genom kommittéförfarande beslutas om ett undantag för kravet på upprättande av en säkerhetsplan (artikel 5.2). Bestämmelserna i Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd anses vara likvärdiga med kravet på säkerhetsplanen.

När en operatör eller ägare har sammanställt sin säkerhetsplan skall denna sändas in till den behöriga myndigheten i medlemsstaten. Varje medlemsstat kommer att inrätta ett uppföljningssystem för dessa säkerhetsplaner, bl.a. för att se till att varje ägare eller operatör får feedback i fråga om planens kvalitet, i synnerhet i fråga om bedömningen av risker och hotbild.

Artikel 6 – Sambandsansvariga i säkerhetsfrågor. Enligt artikel 6 skall alla ägare eller operatörer av europeisk kritisk infrastruktur utse en sambandsansvarig i säkerhetsfrågor. Den

sambandsansvarige skall fungera som en kontaktpunkt i säkerhetsfrågor för att underlätta dialogen mellan de ansvariga för den kritiska infrastrukturen och de nationella myndigheter som är ansvariga för att skydda sådan infrastruktur. Den sambandsansvarige skulle därmed ta emot all information som rör skydd av kritisk infrastruktur från medlemsstatens myndigheten, och skulle omvänt förse myndigheterna med alla relevanta uppgifter om den aktuella infrastrukturen.

Artikel 7 – Rapporteringskraven fastställs i artikel 8. Varje medlemsstat måste således genomföra en bedömning av risker och hotbild i fråga om europeisk kritisk infrastruktur. Dessa uppgifter skall sedan ligga till grund för den uppföljning som avses i artikel 5, dvs. dialogen om säkerhetsfrågor mellan medlemsstaten och de ansvariga för en europeisk kritisk infrastruktur. Enligt artikel 5 krävs det att varje ägare eller operatör av sådan infrastruktur skall utarbeta en egen säkerhetsplan, och lämna in denna till den berörda medlemsstatens myndigheter. Medlemsstaterna ombeds också att utifrån dessa uppgifter sammanställa en allmän översikt över de svagheter, risker och hot som kännetecknar varje berörd sektor, och vidarebefordra denna information till kommissionen. Utifrån dessa uppgifter skall kommissionen sedan avgöra huruvida det behövs ytterligare skyddsåtgärder. Informationen kan också användas i samband med de konsekvensanalyser som görs i samband med eventuella framtida lagförslag inom området.

I artikeln anges också möjligheten att utveckla gemensamma metoder för bedömning av de risker, hot och svagheter som belastar denna infrastruktur. Sådana gemensamma metoder kommer i så fall att antas genom kommittéförfarande.

Artikel 8 – Kommissionens stöd till europeisk kritisk infrastruktur. Kommissionen kommer att stödja ägare och operatörer av europeisk kritisk infrastruktur genom att förmedla god praxis och lämpliga metoder för skydd av sådan infrastruktur. Kommissionen kommer att åta sig att samla in sådan uppgifter från olika källor (tips från medlemsstater, egna förslag osv.) och göra dem tillgängliga för övriga berörda parter.

Artikel 9 – Kontaktpunkter för frågor om skydd av kritisk infrastruktur. För att underlätta samarbete och samordning i fråga om skyddet av kritisk infrastruktur skall varje medlemsstat utse en särskild kontaktpunkt för dessa frågor. Kontaktpunktens funktion blir först och främst att samordna dessa skyddsfrågor inom medlemsstaten, med övriga medlemsstater samt med kommissionen.

Artikel 10 – Hantering av konfidentiella uppgifter i samband med utbyte av information om skydd av kritisk infrastruktur. I arbetet med att skydda kritisk infrastruktur är såväl informationsutbytet som frågan om hantering av konfidentiella uppgifter av stor vikt. Enligt direktivet skall därför både medlemsstaterna och kommissionen vidta lämpliga åtgärder för att skydda information. All personal som hanterar sekretessbelagda uppgifter skall ha säkerhetsprövats på lämpligt sätt av medlemsstatens myndigheter.

Artikel 11 – Kommittéförfaranden. Vissa av direktivets bestämmelser kommer att genomföras genom kommittéförfaranden. Kommittén kommer att bestå av företrädare för de tidigare nämnda kontaktpunkterna för skyddsfrågor. Det rådgivande förfarandet kommer att användas för artikel 5.2, dvs. frågan om undantag av vissa sektorer från kravet att en säkerhetsplan måste utarbetas.

Regleringsförfarandet bör användas för följande åtgärder:

- Artikel 3.1 – Antagande av de övergripande och sektorsspecifika kriterierna för kartläggning av europeisk kritisk infrastruktur.

- Artikel 3.2 – Ändringar i förteckningen över sektorer som omfattar kritisk infrastruktur (bilaga I).

- Artikel 4.2 – Antagande av den preliminära förteckningen över europeisk kritisk infrastruktur.

- Artikel 5.2 – Utveckling av sektorsspecifika krav i fråga om säkerhetsplaner.

- Artikel 7.2 – Utarbetande av en gemensam mall för allmänna rapporter om fastställande av risker, hot och sårbarhet.

- Artikel 7.4 – Utveckling av gemensamma metoder för bedömningar av risker, hot och sårbarhet.

2006/0276 (CNS)

Förslag till

RÅDETS DIREKTIV

om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna

(Text av betydelse för EES)

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 308,

med beaktande av fördraget om upprättandet av Europeiska atomenergigemenskapen, särskilt artikel 203,

med beaktande av kommissionens förslag[1],

med beaktande av Europaparlamentets yttrande[2],

med beaktande av Europeiska centralbankens yttrande[3], och

av följande skäl:

(1) Europeiska rådet uppmanade i juni 2004 till förberedelser för en övergripande strategi för förstärkt skydd av kritisk infrastruktur[4]. Med anledning av detta antog kommissionen den 20 oktober 2004 meddelandet Skydd av viktig infrastruktur i kampen mot terrorismen[5] med förslag om vad som skulle kunna förbättra de förebyggande åtgärderna, beredskapen och insatserna i Europa gentemot terrorattacker som drabbar kritisk infrastruktur.

(2) Den 17 november 2005 antog kommissionen en grönbok om ett europeiskt program för skydd av kritisk infrastruktur[6], där det bland annat redovisas olika åtgärder för att nätverk för varningar om hot mot kritiska infrastrukturer (Critical Infrastructure Warning Information Network, CIWIN). Reaktionerna på grönboken visade tydligt att det finns ett behov av att skapa gemensamma ramar för skydd av kritisk infrastruktur. Man medgav således behovet av att stärka kapaciteten att skydda kritisk infrastruktur i Europa och att minska denna infrastrukturs sårbarhet. Vidare underströks vikten av att följa subsidiaritetsprincipen och föra dialog med berörda parter.

---

1 EUT C […], […], s. […].
2 EUT C […], […], s. […].
3 EUT C […], […], s. […].
4 Rådets dokument 10679/2/04 REV 2.
5 KOM(2004) 702.
6 KOM(2005) 576.

(3) I december 2005 uppmanade rådet (rättsliga och inrikes frågor) kommissionen att lägga fram ett förslag till europeiskt program för skydd av kritisk infrastruktur, och beslutade att detta program generellt skulle vara inriktat på att möta alla typer av risker, även om terrorhot skulle ges högst prioritet. Enligt detta arbetssätt skall såväl hot som orsakas av människor som hot av tekniska karaktär och naturkatastrofer alla omfattas av strategin för skydd av kritisk infrastruktur, även om terrorhotet tillmäts störst vikt. Om det inom en viss sektor som omfattar kritisk infrastruktur bedöms finnas ett tillräckligt gott skydd mot ett enskilt, allvarligt hot, skall berörda parter koncentrera arbetet på andra hot där infrastrukturen fortfarande är sårbar.

(4) För närvarande vilar huvudansvaret för skydd av kritisk infrastruktur på medlemsstaterna och på den enskilda infrastrukturens ägare eller operatör. Detta förhållande bör inte ändras.

(5) Inom gemenskapen finns en rad infrastrukturer vid vilka en driftstörning eller förstörelse skulle drabba två eller flera medlemsstater, eller där en annan medlemsstat skulle drabbas om infrastruktur belägen i en viss medlemsstat utsattes för driftstörningar eller förstörelse. Detta kan också omfatta gränsöverskridande och sektorsövergripande effekter som följer av det inbördes beroende som kännetecknar sammankopplade infrastrukturnät. Sådan infrastruktur (”europeisk kritisk infrastruktur”) bör kartläggas och klassificeras genom ett gemensamt förfarande. Behovet av stärkt skydd för sådan kritisk infrastruktur bör också bedömas enligt gemensamma ramar. En väletablerad och effektiv metod för att skydda gränsöverskridande kritisk infrastruktur är de bilaterala program som inrättats för ändamålet. Det europeiska programmet för skydd av kritisk infrastruktur bör bygga vidare på detta samarbete.

(6) Eftersom det inom vissa sektorer finns särskilda erfarenheter, sakkunskap och behov med avseende på skyddet av kritisk infrastruktur, bör EU vid utvecklingen och genomförandet av en gemensam strategi för skydd av sådan infrastruktur beakta särdragen inom olika sektorer och utgå från de åtgärder som redan vidtagits på EU-nivå, nationellt och regionalt och i sådana fall där ägare eller operatörer av kritisk infrastruktur redan ingått avtal om ömsesidigt stöd över nationsgränserna. Med tanke på den privata sektorns viktiga roll i fråga om övervakning och hantering av risker, avbrottsplanering och återhämtning efter katastrofer måste gemenskapen uppmuntra till ett omfattande engagemang från den privata sektorn. Man behöver sammanställa en gemensam förteckning över sektorer där det finns kritisk infrastruktur, så att den sektorsvisa indelningen av arbetet kan fungera.

(7) Varje ägare eller operatör av europeisk kritisk infrastruktur bör upprätta en säkerhetsplan, där man kartlägger kritiska anläggningar och redogör för de säkerhetslösningar som används för att skydda dessa. Säkerhetsplanen skall bygga på bedömningar av risker, hot och svagheter, samt på andra relevanta uppgifter som lagts fram av medlemsstaternas myndigheter.

(8) Varje ägare eller operatör av kritisk infrastruktur bör utse en sambandsansvarig i säkerhetsfrågor, med uppgift att underlätta samarbete och kommunikation med berörda nationella myndigheter med ansvar för skydd av kritisk infrastruktur.

(9) En effektiv kartläggning av risker, hot och sårbarhet inom enskilda sektorer kräver att en god kommunikation upprätthålls mellan ägare och operatörer av europeisk kritisk

infrastruktur och medlemsstaterna, liksom mellan medlemsstaterna och kommissionen. Varje medlemsstat bör samla in information om europeisk kritisk infrastruktur på sitt eget territorium. Kommissionen bör få del av allmän information om sårbarhet, hot och risker – där så är lämpligt även uppgifter om eventuella luckor i säkerheten och om beroende mellan olika sektorer – såsom ett underlag för enskilda förslag till att i nödvändiga fall förbättra skyddet av europeisk kritisk infrastruktur.

(10) För att underlätta förbättringar av europeisk kritisk infrastruktur bör det införas gemensamma metoden för att kartläggning och klassificering av de svagheter, hot och risker som kan drabba sådan infrastruktur.

(11) Gemensamma ramar är nödvändiga för att kunna genomföra väl samordnade åtgärder till skydd för europeisk kritisk infrastruktur, och för att kunna göra en tydlig distinktion mellan de olika berörda parternas ansvarsområden. Ägare och operatörer av europeisk kritisk infrastruktur bör utbyta information om god praxis och framgångsrika metoder när det gäller skydd av sådan infrastruktur.

(12) För att skyddet av kritisk infrastruktur skall bli effektivt krävs kommunikation, samordning och samarbete på nationell nivå och gemenskapsnivå. Detta uppnås bäst genom att man inrättar särskilda kontaktpunkter för skyddsfrågor i varje medlemsstat. Syftet med dessa kontaktpunkter bör vara att samordna frågor som rör skydd av kritisk infrastruktur, såväl internt som i förhållande till andra medlemsstater och till kommissionen.

(13) För att skyddet av kritisk infrastruktur skall kunna utvecklas även på områden där det krävs en viss grad av sekretess bör man inom ramen för detta direktiv skapa former för att samordna och insynsskydda informationsutbytet. Vissa uppgifter som rör skydd av kritisk infrastruktur är av sådan art att en vidare spridning skulle skada allmänintresset och den allmänna säkerheten. Särskilda uppgifter om kritiska infrastrukturanläggningar, som skulle kunna underlätta planering och genomförande av handlingar som skapar oacceptabel skada på dessa anläggningar, bör vara sekretessbelagda och tillgång till dessa uppgifter bör endast ges till de parter på nationell nivå och gemenskapsnivå som måste känna till dem.

(14) Utbytet av uppgifter om kritisk infrastruktur bör ske i en anda av förtroende och med en god säkerhetsnivå. Informationsutbudet förutsätter att företag och organisationer kan lita på att de känsliga uppgifter de bidrar med kommer att skyddas på ett fullgott sätt. För att uppmuntra till utbytet bör de berörda parterna inom näringslivet också kunna vara förvissade om att fördelarna med att dela med sig av information om kritisk infrastruktur är större än kostnaderna för näringslivet och för samhället som helhet. Informationsutbyte om kritisk infrastruktur bör därför uppmuntras.

(15) Detta direktiv utgör ett komplement till de sektorsbestämmelser som antagits på gemenskapsnivå och i medlemsstaterna. De gemenskapsmekanismer som redan införts bör fortsätta att utnyttjas, och kommer att bidra till det övergripande genomförandet av direktivet.

(16) De bestämmelser som krävs för att genomföra direktivet bör antas i enlighet med rådets direktiv 1999/468/EG av den 28 juni 1999 om de förfaranden som skall tillämpas vid utövandet av kommissionens genomförandebefogenheter[7].

(17) Åtgärder från medlemsstaternas sida räcker inte för att på ett tillfredsställande sätt uppnå målet med detta direktiv, nämligen att inrätta ett förfarande för kartläggning och klassificering europeisk kritisk infrastruktur och en gemensam metod för att bedöma behovet av förbättring av denna infrastruktur. Med tanke på uppgiftens omfattning kan därför detta mål bättre uppnås genom åtgärder på gemenskapsnivå, och gemenskapen bör därför kunna vidta åtgärder i enlighet med den subsidiaritetsprincip som fastställs i artikel 5 i fördraget. Med tanke på proportionalitetsprincipen, som också fastställs i samma artikel, går bestämmelserna i detta direktiv inte utöver vad som är nödvändigt för att uppnå de uppsatta målen.

(18) Direktivets bestämmelser har formulerats i överensstämmelse med de grundläggande rättigheter som bland annat bekräftas i Europeiska unionens stadga om de grundläggande rättigheterna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1
Syfte

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

Artikel 2
Definitioner

I detta direktiv gäller följande definitioner:

a) *kritisk infrastruktur*: anläggningar eller delar av dessa som är nödvändiga för att upprätthålla centrala samhällsfunktioner, såsom försörjningskedjan och funktioner som rör hälsa, säkerhet, försörjningstrygghet och människors ekonomiska eller sociala välfärd.

b) *europeisk kritisk infrastruktur*: kritisk infrastruktur som vid driftstörning eller förstörelse skulle få betydande följder för två eller fler medlemsstater, eller en enskild medlemsstat om den kritiska infrastrukturen finns i en annan medlemsstat. Detta inbegriper effekter till följd av sektorsöverskridande beroende av andra typer av infrastruktur.

c) *konsekvensernas allvar*: driftstörningens eller förstörelsens inverkan på en viss infrastruktur med avseende på

[7] EGT L 184, 17.7.1999, s. 23.

- inverkan på allmänheten (antal personer i befolkningen som påverkas),
- ekonomisk effekt (den ekonomiska förlustens betydelse eller försämringen av produkter eller tjänster),
- effekter för miljön, och
- politiska effekter.
- psykologiska effekter.
- effekter på folkhälsan.

d) *sårbarhet*: ett särdrag i en del av den kritiska infrastrukturens utformning, funktion eller drift som gör den känslig för driftstörning eller förstörelse genom ett hot och dessutom är beroende av andra typer av infrastruktur.

e) *hot*: indikation, omständighet eller händelse som potentiellt kan störa eller förstöra kritisk infrastruktur eller någon del av denna.

f) *risk*: risken för förlust eller skada med avseende på det värde som ägaren eller operatören sätter på tillgången och effekten av en förlust eller förändring av tillgången samt sannolikheten att en viss sårbarhet kommer att utnyttjas för ett viss typ av hot.

g) *uppgifter om skydd av kritisk infrastruktur*: specifika uppgifter om kritisk infrastruktur som, om de avslöjades, skulle kunna användas till att planera och agera för att bädda för haveri eller förorsaka oacceptabla följder för kritisk infrastruktur.

Artikel 3
Kartläggning av europeisk kritisk infrastruktur

1. De övergripande och sektorspecifika kriterier som skall tillämpas för att kartlägga europeiska kritiska infrastrukturer antas i enlighet med det förfarande som avses i artikel 11.3. Kriterierna får ändras i enlighet med förfarandet i artikel 11.3.

   De övergripande kriterier som skall tillämpas på alla infrastruktursektorer skall utvecklas med hänsyn till hur allvarliga effekterna blir om viss infrastruktur utsätts för driftstörningar eller förstörs. De skall ha antagits senast den [*ett år efter det att direktivet trätt i kraft*].

   De sektorspecifika kriterierna skall utvecklas för prioriterade sektorer samtidigt som hänsyn tas till utmärkande drag för enskilda individuella kritiska infrastruktursektorer och när så är lämpligt inbegripa berörda parter. De skall antas för varje prioriterad sektor senast ett år efter det att den definierats som en prioriterad sektor.

2. Bland de sektorer som förtecknas i bilaga I skall kommissionen på årsbasis utse vilka prioriterade sektorer som skall användas för att utveckla de kriterier som föreskrivs i punkt 1.

Bilaga I kan ändras i enlighet med det förfarande som avses i artikel 11.3 så länge detta inte vidgar direktivets giltighetsområde.

3. Varje medlemsstat skall kartlägga både kritiska infrastrukturer som finns på det egna territoriet och kritiska infrastrukturer utanför dess territorium som kan påverka den och som uppfyller de kriterier som antagits med stöd i punkterna 1 och 2.

Varje medlemsstat skall senast ett år efter antagandet av relevanta kriterier och därefter fortlöpande meddela kommissionen om vilka kritiska infrastrukturer som kartlagts på detta sätt.

Artikel 4
Klassificering av europeisk kritisk infrastruktur

1. På grundval av de meddelanden som inkommit enligt artikel 3.3 andra stycket och all annan tillgänglig information skall kommissionen lägga fram en förteckning över kritiska infrastrukturer som skall klassificeras som europeiska kritiska infrastrukturer.

2. Förteckningen över kritiska infrastrukturer klassificerade som europeisk kritisk infrastruktur skall antas i enlighet med det förfarande som avses i artikel 11.3.

Förteckningen får ändras i enlighet med förfarandet i artikel 11.3.

Artikel 5
Säkerhetsplaner

1. Varje medlemsstat skall kräva att ägarna eller operatörerna av varje europeisk kritisk infrastruktur på det egna territoriet upprättar och uppdaterar en säkerhetsplan och se över den minst vartannat år.

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

I enlighet med det förfarande som avses i artikel 11.2 kan kommissionen besluta att förenligheten med åtgärder tillämpliga på specifika sektorer som förtecknas i bilaga I uppfyller kravet att utarbeta och uppdatera en säkerhetsplan.

3. Den europeiska kritiska infrastrukturens ägare eller operatör skall lämna in säkerhetsplanen till den berörda myndigheten i medlemsstaten inom ett år efter klassificeringen av den kritiska infrastrukturen som europeisk kritisk infrastruktur.

I de fall där specifika krav avseende säkerhetsplanen har antagits på grundval av punkt 2 behöver inte säkerhetsplanen lämnas in till den berörda medlemsstatens myndigheter förrän ett år efter antagandet av de sektorsspecifika kraven.

4. Varje medlemsstat skall inrätta ett system som garanterar adekvat och regelbunden översyn av säkerhetsplanerna och genomförandet av dess grundat på de risk- och hotanalyser som gjorts enligt artikel 7.1.

5. Efterlevnaden av Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd uppfyller kraven för att upprätta en säkerhetsplan.

Artikel 6
Sambandsansvariga i säkerhetsfrågor

1. Varje medlemsstat skall kräva att ägarna eller operatörerna av europeiska kritiska infrastrukturer på det egna territoriet att utse en sambandsansvarig i säkerhetsfrågor som kontaktpunkt för säkerhetsfrågor mellan ägaren eller operatören av infrastrukturen och medlemsstaternas berörda myndigheter med ansvar för infrastrukturskydd. Den sambandsansvarige i säkerhetsfrågor skall utses inom ett år efter klassificeringen av den kritiska infrastrukturen som en europeisk kritisk infrastruktur.

2. Varje medlemsstat skall meddela den sambandsansvarige om relevant information avseende kartlagda risker och hot som gäller den berörda europeiska kritiska infrastrukturen.

Artikel 7
Rapportering

1. Varje medlemsstat skall genomföra en risk- och hotbedömning med avseende på europeisk kritisk infrastruktur på dess eget territorium inom ett år efter klassificeringen av den kritiska infrastrukturen som europeisk kritisk infrastruktur.

2. Varje medlemsstat skall sammanfattningsvis rapportera till kommissionen om vilka typer av sårbarhet, hot och risker som man stöter på i varje sektor som avses i bilaga I inom 18 månader efter antagandet av den förteckning som föreskrivs i artikel 4.2 och därefter fortlöpande vartannat år.

   En gemensam mall för rapporterna skall utvecklas enligt förfarandet i artikel 11.3.

3. Kommissionen skall sektorsvis bedöma om det krävs några specifika skyddsåtgärder för europeiska kritiska infrastrukturer.

4. Gemensamma metoder för att göra sårbarhets-, risk- och hotbedömningar med avseende på europeiska kritiska infrastrukturer kan utvecklas sektorsvis enligt förfarandet i artikel 11.3.

Artikel 8
Kommissionens stöd för europeiska kritiska infrastrukturer

Kommissionen skall stödja ägarna eller operatörerna av klassificerade europeiska kritiska infrastrukturer genom att ge dem tillgång till bästa praktiker och metoder för att skydda kritisk infrastruktur.

Artikel 9
Kontaktpunkter för frågor om skydd kritisk infrastruktur

1. Varje medlemsstat skall utse en kontaktpunkt för skyddet av kritisk infrastruktur.

2. Kontaktpunkten skall samordna frågor som rör skyddet av kritisk infrastruktur inom medlemsstaten, med andra medlemsstater och med kommissionen.

Artikel 10
Sekretess och utbyte av information om skydd av kritiska infrastrukturer

1. Vid tillämpningen av denna förordning skall kommissionen, i enlighet med beslut 2001/844/EG, EKSG, Euratom, vidta lämpliga åtgärder för att skydda sekretessbelagd information som den har tillgång till, eller som medlemsstaterna har lämnat till kommissionen. Medlemsstaterna skall vidta likvärdiga åtgärder i enlighet med gällande nationell lagstiftning. Lämpliga hänsyn skall tas till potentiella nackdelar för gemenskapens eller en eller flera av dess medlemsstaters centrala intressen.

2. Varje person som åt en medlemsstat hanterar uppgifter som enligt detta direktiv är hemliga skall ha genomgått lämplig säkerhetsprövning.

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

Artikel 11
Kommitté

1. Kommissionen skall bistås av en kommitté som är sammansatt av företrädare för varje kontaktpunkt för frågor om skyddet av kritisk infrastruktur.

2. När det hänvisas till denna punkt skall artiklarna 3 och 7 i beslut 1999/468/EG tillämpas, med beaktande av bestämmelserna i artikel 8 i beslutet.

3. När det hänvisas till denna punkt skall artiklarna 5 och 7 i beslut 1999/468/EG tillämpas, med beaktande av bestämmelserna i artikel 8 i beslutet.

   Den tid som avses i artikel 5.6 i beslut 1999/468/EG skall vara en månad.

4. Kommittén skall själv anta sin arbetsordning.

Artikel 12
Genomförande

1. Medlemsstaterna skall anta de lagar och andra förordningar som är nödvändiga för att följa detta direktiv senast den 31 december 2007. De skall genast överlämna texterna till dessa bestämmelser till kommissionen tillsammans med en jämförelsetabell för dessa bestämmelser och bestämmelserna i detta direktiv.

När medlemsstaterna antar dessa bestämmelser skall de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen skall göras utfärdas av varje medlemsstat själv.

2. Medlemsstaterna skall till kommissionen överlämna texten till de centrala bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

Artikel 13
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 14
Adressater

Detta direktiv riktar sig till samtliga medlemsstater.

Utfärdat i Bryssel den [...]

På rådets vägnar

BILAGA I

FÖRTECKNING ÖVER SEKTORER MED KRITISK INFRASTRUKTUR

Sektor		Delsektor	
I	Energi	1	Olje- och gasproduktion, raffinaderier, behandling, lagring och distribution i rörledningar
		2	Produktion och överföring av el
II	Kärnindustri	3	Produktion och lagring eller processning av kärnämnen
III	Informations- och kommunikationsteknik	4	Skydd av informationssystem och nätverk
		5	System för instrumentautomation och övervakning (SCADA osv.)
		6	Internet
		7	Fast telefoni
		8	Mobil telefoni
		9	Radiokommunikation och navigation
		10	Satellitkommunikation
		11	Radio- och TV-utsändningar
IV	Vatten	12	Dricksvattensförsörjning
		13	Kontroll av vattenkvalitet
		14	Uppdämning och kontroll av vattenmängder
V	Livsmedel	15	Livsmedelsförsörjning och garantier för livsmedelssäkerhet och livsmedelsförsörjning
VI	Hälso- och sjukvård	16	Sjukhusvård och sjukvård
		17	Mediciner, serum, vacciner och läkemedel
		18	Biologiska laboratorier och biologiska ämnen
VII	Finans	19	Clearing- och avvecklingssystem för betalningar och värdepapper samt tillhörande system
		20	Reglerade marknader
VIII	Transporter	21	Vägtransporter
		22	Järnvägar
		23	Lufttransporter
		24	Transporter på inre vattenvägar
		25	Havs- och närsjöfart
IX	Kemisk industri	26	Produktion och lagring eller processning av kemiska ämnen
		27	Rörledningar för farliga ämnen (kemiska ämnen)
X	Rymdforskning	28	Rymdforskning
XI	Forskningsanläggningar	29	Forskningsanläggningar

BILAGA II

SÄKERHETSPLAN

Säkerhetsplanen skall kartlägga ägarna och operatörerna av de anläggningar som definieras som kritisk infrastruktur och inrätta lämpliga säkerhetslösningar för att skydda dem. Säkerhetsplanen måste minst omfatta följande:

– Kartläggning av viktiga anläggningar.

– En riskanalys som bygger på scenarier över betydande hot, anläggningarnas sårbarhet och potentiella effekter.

– Kartläggning, urval och prioritering av motåtgärder och förfaranden med en uppdelning följande två undergrupper:

- **Permanenta säkerhetsåtgärder**, kartläggning av oundgängliga säkerhetsinvesteringar och medel som inte kan installeras av ägare eller operatörer med kort varsel. Rubriken skall innehålla information om allmänna åtgärder, tekniska åtgärder (bl.a. installation av detektorer, inpasseringskontroll, skydd och förebyggande åtgärder), organisatoriska åtgärder (bl.a. förfaranden för varningar och krishantering), kontroll- och verifieringsåtgärder, kommunikation, ökad medvetenhet och utbildning samt systemsäkerhet.

- **Graderade säkerhetsåtgärder**, som aktiveras beroende på varierande risk- och hotnivåer.

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

Politikområde: Rättsliga och inrikes frågor

Verksamhet: Skydd av kritisk infrastruktur

ÅTGÄRDENS BETECKNING: Rådets direktiv om kartläggning och definiering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna

1. BERÖRDA BUDGETRUBRIKER

EJ TILLÄMPLIGT

2. ALLMÄNNA UPPGIFTER

2.1. Sammanlagda anslag för åtgärden (del B): miljoner euro i åtagandebemyndiganden

EJ TILLÄMPLIGT

2.2. Tillämpningsperiod:

Börjar 2006

2.3. Flerårig total utgiftsberäkning:

a) Förfalloplan för åtagandebemyndiganden/betalningsbemyndiganden (ekonomiskt stöd) (*se punkt 6.1.1)*

Miljoner euro (*avrundat till tre decimaler*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Totalt
Åtagandebemyndiganden	-	-	-	-	-	-	-
Betalningsbemyndiganden	-	-	-	-	-	-	-

b) Tekniskt och administrativt stöd samt stödutgifter *(se punkt 6.1.2)*

Åtagandebemyndiganden	-	-	-	-	-	-	-
Betalningsbemyndiganden	-	-	-	-	-	-	-

Delsumma a+b	-	-	-	-	-	-	-

Åtagandebemyndiganden	-	-	-	-	-	-	-
Betalningsbemyndiganden	-	-	-	-	-	-	-

c) Total budgetkonsekvens i form av personalutgifter och övriga administrativa utgifter *(se punkterna 7.2 och 7.3)*

Åtagandebemyndiganden och betalningsbemyndigande n	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000

TOTALT a+b+c	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000
Åtagandebemyndiganden	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000
Betalningsbemyndigande n	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000	1 280 000

2.4. Förenlighet med den ekonomiska planeringen och budgetplanen

Direktivet är förenligt med programmet Terrorism – förebyggande, beredskap och konsekvenshantering samt andra säkerhetsrelaterade risker för perioden 2007–2013.

2.5. Påverkan på inkomsterna:

Det nyligen antagna programmet Terrorism – förebyggande, beredskap och konsekvenshantering samt andra säkerhetsrelaterade risker för perioden 2007–2013 (137,5 miljoner euro) kommer, som en del av det allmänna programmet Säkerhet och skydd av friheter att bidra till genomförandet av det europeiska programmet för skydd av kritiska infrastrukturer mot säkerhetsrisker och skyddet av sådana fysiska resurser, tjänster och it-anläggningar samt nätverk och infrastrukturanläggningar som, om de utsätts för störningar eller förstörs, allvarligt skulle påverka samhällets kritiska funktioner. Programmets omfattning är begränsad eftersom det inte täcker investeringar i hårdvara och utrustning. Detta program gäller inte områden som omfattas av andra finansiella instrument, särskilt snabbinsatsinstrumentet i fall av stora olyckor.

När det gäller förebyggande av och beredskap för terrorattacker syftar programmet till att

a) stimulera, främja och stödja risk- och hotbedömningar av kritisk infrastruktur, även genom utvärderingar på plats, för att kartlägga möjliga hot och sårbara punkter samt behov av att uppgradera deras säkerhet,

b) främja och stödja gemensamma operativa insatser för att förbättra säkerheten i de gränsöverskridande försörjningskedjorna, förutsett att konkurrensreglerna på den inre marknaden inte snedvrids,

c) främja och stödja utvecklingen av lägsta säkerhetsnivåer, utbyte av bästa praxis, riskbedömningsverktyg, metoder för att jämföra och prioritera

infrastruktur inom olika sektorer, sårbarhetsanalys samt inbördes beroende i fråga om skydd av infrastruktur,

d) främja och stödja EU-omfattande samordning och samarbete i fråga om skydd av kritisk infrastruktur. I tillämpliga fall utveckling av förslag till lägsta skyddsåtgärder och gemensamma riktlinjer.

När det gäller förebyggande av och beredskap för terrorattacker syftar programmet till att

a) stimulera, främja och stödja utbyte av praktisk kunskap, erfarenhet och teknik,

b) stimulera, främja och stödja utveckling av lämpliga metoder och beredskapsplaner, och

c) säkerställa omedelbart expertstöd, när det gäller säkerhetsfrågor inom övergripande system för krishantering, förvarning och räddningstjänst.

Förslaget påverkar därför inte inkomsterna.

3. BUDGETTEKNISKA UPPGIFTER

Typ av utgifter		Nya	Bidrag från Efta-länder	Bidrag från kandidatländer	Rubrik i budgetplanen
Icke-oblig. utg.	Icke-diff.	EJ TILLÄMPLIGT	EJ TILLÄMPLIGT	EJ TILLÄMPLIGT	Ej tillämpligt

4. RÄTTSLIG GRUND

Den rättsliga grunden för förslaget är artikel 308 i fördraget om upprättandet av Europeiska gemenskapen.

5. BESKRIVNING AV OCH SKÄL FÖR ÅTGÄRDEN

5.1. Behovet av gemenskapsåtgärder

5.1.1. Mål

Ett direktiv är det bästa sättet att skapa en ram för ett europeiskt program för skydd av kritisk infrastruktur, eftersom medlemsstaterna har olika metoder för skydd av kritisk infrastruktur och olika rättsliga traditioner. Genom att framhålla ett antal centrala idéer och låta medlemsstaterna tillämpa de metoder som bäst passar deras behov, kan målen med det europeiska programmet för skydd av kritiska infrastrukturer förverkligas genom att man bygger på vad som redan uppnåtts.

5.1.2. Åtgärder som vidtagits till följd av förhandsutvärderingar

Alla berörda parter har rådfrågats om utvecklingen av det europeiska programmet för skydd av kritiska infrastrukturer. Detta har gjorts på följande sätt:

- Grönboken om inrättandet av ett europeiskt program för skydd av kritisk infrastruktur antogs den 17 november 2005 med en samrådsperiod som slutar den 15 januari 2006. 22 medlemsstater inkom med officiella svar under samrådsperioden. Omkring hundra företrädare för den privata sektorn inkom också med synpunkter på grönboken. Svaren gav ett generellt stöd för idén att inrätta ett europeiskt program för skydd av kritisk infrastruktur.

- Kommissionen stod värd för tre seminarier om skydd av kritisk infrastruktur (i juni 2005, september 2005 och mars 2006). I samtliga tre seminarier deltog företrädare för medlemsstaterna. Den privata sektorn inbjöds till seminarierna i september 2005 och mars 2006.

- Informella möten för kontaktpunkter för frågor om skydd av kritisk infrastruktur. Kommissionen stod värd för två möten med kontaktpunkterna för frågor om skydd av kritisk infrastruktur (december 2005 och februari 2006).

- Informella möten med företrädare för den privata sektorn. Talrika informella möten hölls med företrädare för såväl enskilda privata företag som branschorganisationer.

- Inom kommissionen fördes arbetet med att utveckla det europeiska programmet om skydd för kritiska infrastrukturer framåt med hjälp av regelbundna möten i gruppen för frågor som rör skydd av kritisk infrastruktur som är en interinstitutionell undergrupp till gruppen för frågor som rör interna aspekter av terrorismen.

5.2. Planerad verksamhet och villkor för finansiering via budgeten

En uppskattning av budgeteffekterna lämnas i den bifogade finansieringsöversikten.

5.3. Genomförandemetoder

Eftersom det rör sig om ett direktiv krävs ingen särskild metod för budgetgenomförandet.

6. BUDGETKONSEKVENSER

6.1. Totala budgetkonsekvenser för del B (för hela programperioden)

6.1.1. Ekonomiskt stöd

EJ TILLÄMPLIGT

6.1.2. Tekniskt och administrativt stöd, stödutgifter och IT-utgifter (åtagandebemyndiganden)

EJ TILLÄMPLIGT

6.2. Kostnadsberäkning per åtgärd för del B (för hela programtiden)

EJ TILLÄMPLIGT

7. EFFEKTER PÅ PERSONALRESURSER OCH ADMINISTRATIVA UTGIFTER

7.1. Effekter på personalresurserna

Typ av tjänster		Personal som krävs för att förvalta åtgärden (befintliga plus ev. ytterligare personalresurser)		Totalt	Beskrivning av de arbetsuppgifter som den planerade åtgärden för med sig
		Antal fasta tjänster	Antal tillfälliga tjänster		
Tjänstemän eller tillfälligt anställda	A B C	8 A 1 B	1 C	10	Insamling och behandling av information som förberedelse för kommittémötena
Övriga personalresurser					
Totalt		9	1	10	

Behovet av personalresurser och administrativa resurser skall täckas inom ramen för de anslag som beviljats det generaldirektorat som ansvarar för åtgärden i samband med den årliga anslagstilldelningen.

7.2. Total budgetkonsekvens av personalresurserna

Typ av personal	Belopp (euro)	Beräkningsmetod*
Tjänstemän Tillfällig personal	1 080 000 48 000	(108 000 x 10 = 1 080 000 4 000 x 12 = 48 000
Övriga personalresurser (ange budgetrubrik)		
Totalt	1 128 000	

Beloppen avser totala utgifter för 12 månader.

7.3. Övriga administrativa utgifter till följd av åtgärden

Budgetrubrik (nummer och benämning)	Belopp i euro	Beräkningsmetod
Totalt (avdelning A7)		
A0701 – Tjänsteresor	24 000	2000 x 12 månader = 24 000
A07030 – Möten	-	-
A07031 - Kommittéer vars hörande är obligatoriskt	128 000	32 000 x 4 möten om året = 128 000
A07032 - Kommittéer vars hörande ej är obligatoriskt	-	-
A07040 – Konferenser m.m.	-	-
A0705 – Studier och samråd	-	-
Övriga utgifter (ange vilka)		
Informationssystem (A-5001/A-4300)	-	-
Övriga utgifter i del A (ange vilka)		
Totalt	152 000	

Beloppen avser totala utgifter för 12 månader.

Ange vilken typ av kommitté som avses samt vilken grupp den tillhör.

I.	Totalbelopp/år (tabell 7.2 + 7.3)	1 280 000
II.	Varaktighet	Pågående
III.	Sammanlagd kostnad för åtgärden (I x II)	

8. ÖVERVAKNING OCH UTVÄRDERING

8.1. Övervakning

EJ TILLÄMPLIGT

8.2. Planerad form och tidsplan för utvärderingen

EJ TILLÄMPLIGT

9. BESTÄMMELSER OM BEDRÄGERIBEKÄMPNING

EJ TILLÄMPLIGT

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 12.12.2006
SEK(2006) 1648

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

Oheisasiakirja

Ehdotus:

NEUVOSTON DIREKTIIVI

Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta

VAIKUTUSTENARVIOINNIN TIIVISTELMÄ

{KOM(2006) 787 lopullinen}
{SEC(2006) 1654}

VAIKUTUSTENARVIOINNIN TIIVISTELMÄ

Tausta

Euroopan unionin turvallisuus ja talous sekä kansalaisten hyvinvointi perustuvat tiettyihin infrastruktuureihin ja niiden avulla tarjottaviin palveluihin. Keskeisiä palveluita tarjoavien infrastruktuurien vahingoittuminen tai tuhoutuminen voisi aiheuttaa ihmishenkien ja omaisuuden menetyksiä sekä yleisön luottamuksen ja moraalin romahtamisen Euroopan unionissa.

Elintärkeät infrastruktuurit voivat vahingoittua tai tuhoutua monenlaisten joko ihmisen aiheuttamien tai luonnononnettomuuksien vuoksi. Elintärkeiden infrastruktuurien toiminnassa ilmenevät häiriöt tai manipulaatiot tulisi voida rajoittaa mahdollisimman lyhytaikaisiksi, harvoin toistuviksi, hallittaviksi ja maantieteellisesti rajatuiksi, niin että niistä aiheutuu mahdollisimman vähän vahinkoa jäsenvaltioiden, niiden kansalaisten ja koko Euroopan unionin hyvinvoinnille.

Mikä on ongelma?

Ongelmana on Euroopassa sijaitsevien elintärkeiden infrastruktuurien haavoittuvuus ja sitä kautta myös niiden avulla tarjottavien palvelujen haavoittuvuus. Ongelma johtuu osittain siitä, että elintärkeitä infrastruktuureja ei ole kaikissa jäsenvaltioissa suojattu riittävän hyvin, mikä lisää myös muiden jäsenvaltioiden potentiaalista haavoittuvuutta.

Keitä ongelma koskee?

Ongelma voi koskea kaikkia Euroopan unionin alueella asuvia ihmisiä, siellä toimivia liikeyrityksiä, jäsenvaltioiden hallituksia ja koko Euroopan unionia. Vaikutukset voivat olla sekä välittömiä (esim. terrori-iskun uhrit) että välillisiä (esim. palvelujen häiriytyminen niiden perustana olevan infrastruktuurin vahingoittumisen seurauksena).

Miksi tarvitaan kiireellisesti EU:n tason toimia?

- Yhä useammat jäsenvaltiot laativat parhaillaan omia menettelyjään elintärkeiden infrastruktuurien suojaamista varten. Ne odottavat, että komissio esittää elintärkeiden infrastruktuurien suojaamista koskevan EU:n tason ohjelman, jotta ne voivat ottaa EU:n yhteiset toimet huomioon omissa menettelyissään. Jos yhteisen kehyksen laatiminen viivästyy, on vaarana, että jäsenvaltioissa otetaan käyttöön keskenään yhteensopimattomia menettelyjä elintärkeiden infrastruktuurien suojaamista varten.

- Infrastruktuureista on karsittava erityisesti sellaiset ongelmakohdat, joilla voi olla valtioiden rajat ylittäviä vaikutuksia. On minimoitava riski, että jokin jäsenvaltio joutuu kärsimään toimintahäiriöistä siksi, että jokin toinen jäsenvaltio ei ole suojannut infrastruktuuria riittävän hyvin.

- On minimoitava ylimääräiset kustannukset, joita useammassa kuin yhdessä jäsenvaltiossa toimiville yrityksille voi aiheutua sen vuoksi, että niiden on toteutettava monenlaisia turvatoimia.

- Eräät infrastruktuurit, kuten energiaputkistot ja jakeluverkot, ovat yhä enenevässä määrin yleiseurooppalaisia, minkä vuoksi kansalliset toimet eivät yksinään riitä niiden suojaamiseen.

- On selvää, että eräiden Euroopassa sijaitsevien elintärkeiden infrastruktuurien suojaamisen parantamiseen liittyvien yksityiskohtien tutkiminen (esimerkiksi keskinäisten riippuvuussuhteiden selvittäminen) vie aikaa. Siksi työ olisikin saatava alulle mahdollisimman pian, ja sitä olisi tehtävä yhteiseltä pohjalta.

- Sidosryhmien kuuleminen alkoi jo vuonna 2004. Sitä varten on järjestetty kolme EU:n laajuista seminaaria elintärkeiden infrastruktuurien suojaamisesta, laadittu vihreä kirja ja kutsuttu koolle kaksi elintärkeiden infrastruktuurien suojaamisesta vastaavien yhteyspisteiden epävirallista tapaamista ja useita kahdenvälisiä kokouksia hallitusten ja yksityisen sektorin edustajien kesken.

- Rikollisuuden ja terrorismin uhka ei vähene. Jäsenvaltioiden ja komission yhteistyö näiden uhkien torjumiseksi on yhteisen edun mukaista, sillä näin voidaan saavuttaa synergiaetuja.

Tavoite

Ehdotetun politiikan yleisenä tavoitteena on parantaa elintärkeiden infrastruktuurien suojaamista Euroopan unionissa.

Neljän toimintavaihtoehdon hyvät ja huonot puolet

On määritetty eri toimintavaihtoehtoja, joiden avulla edellä mainittu tavoite voitaisiin saavuttaa:

1. Luovutaan elintärkeiden infrastruktuurien suojaamiseen tähtäävien toimien toteuttamisesta Euroopan tasolla. Tämän vaihtoehdon mukaan Euroopan tasolla ei toteuteta lainkaan horisontaalisia toimia tällä alalla.

   Uusien toimien toteuttamatta jättämiseen perustuva vaihtoehto ei edistä elintärkeiden infrastruktuurien suojaamista Euroopassa. Sen sijaan siihen liittyy eräitä haittapuolia, kuten kilpailuongelmat, liikeyrityksille aiheutuvat ylimääräiset kustannukset ja turvallisuusvajeet. Kaikki jäsenvaltiot ovat hylänneet tämän vaihtoehdon. Yleensä ottaen ne katsovat, että elintärkeiden infrastruktuurien suojaamista on syytä käsitellä koko Euroopan näkökulmasta.

2. Vapaaehtoisuuteen perustuva toimintakehys. Tämän vaihtoehdon mukaan laadittaisiin vapaaehtoisuuteen perustuva toimintakehys, jota jäsenvaltiot voisivat soveltaa tai olla soveltamatta valintansa mukaan.

   Vapaaehtoisuuteen perustuvan toimintakehyksen selkeänä etuna on, että luodaan kehys, jonka tarkoituksena on synnyttää luottamusta kaikkien sidosryhmien välille. Tämä ei kuitenkaan riitä tasoittamaan tähän vaihtoehtoon liittyviä mittavia haittoja, joita ovat kustannusten kasvu, kilpailuongelmat ja turvallisuusriskien lisääntyminen. Tämän vaihtoehdon keskeinen ongelma on turvallisuus. Vapaaehtoisuuteen perustuva toimintakehys ei luo toiminnalle perustaa, joka velvoittaisi kaikki jäsenvaltiot suojaamaan elintärkeät infrastruktuurinsa riittävällä tavalla.

3. Kevyt sääntelykehys. Tämän vaihtoehdon mukaan Euroopan tasolla otettaisiin käyttöön joitakin sitovia toimenpiteitä. Jäsenvaltioille asetettaisiin tiettyjä yleisiä velvoitteita, mutta pääpaino olisi edelleen parhaiden käytänteiden vaihdossa, vuoropuhelussa ja luottamuksen lisäämisessä EU:n tasolla.

   Kevyen sääntelykehyksen käyttöönottoon perustuvassa vaihtoehdossa hyödyt ja haitat ovat parhaiten tasapainossa. Tämä menettelytapa turvaa kilpailuedellytysten säilymisen, vähentää useammassa kuin yhdessä jäsenvaltiossa toimivien yritysten kustannuksia ja lisää turvallisuutta Euroopan unionissa. Nämä ovat selkeitä etuja, jotka näyttäisivät kompensoivan kustannuksiin liittyvät haittatekijät. Toinen tähän vaihtoehtoon liittyvä mahdollinen haitta liittyy siihen, että sen myötä EU:ssa otettaisiin käyttöön jälleen uusi sääntelykehys. Turvallisuusnäkökohtien kannalta tämä näyttäisi kuitenkin perustellulta.

4. Toimien täydellinen yhdenmukaistaminen EU:n tasolla. Tämän vaihtoehdon mukaan EU:n tasolla laaditaan ehdotus elintärkeiden infrastruktuurien suojaamiseen liittyvien jäsenvaltioiden toimenpiteiden ja infrastruktuurien omistajia/ylläpitäjiä koskevien turvallisuusnormien täydellisestä yhdenmukaistamisesta.

   Toimien täydellistä yhdenmukaistamista koskeva vaihtoehto sisältää useita selkeitä hyötyjä ja haittoja. Hyödyllistä on se, että EU:n elintärkeät infrastruktuurit saisivat korkeatasoisen suojan. Haittapuolena taas on se, että tästä aiheutuisi huomattavia kustannuksia ja että sidosryhmien välille olisi vaikea rakentaa luottamusta. Jäsenvaltiot ovat jo hylänneet tämän vaihtoehdon, sillä ne haluavat EU:n tason yleisen suojaamisohjelman, jonka pohjalta ne voivat kehittää ja täydentää tähänastisia toimiaan. Täydellistä yhdenmukaistamista edellyttävä vaihtoehto saattaa olla toissijaisuus- ja oikeasuhteisuusperiaatteiden vastainen, ja on erittäin todennäköistä, että jäsenvaltiot torjuisivat sen.

Näiden neljän vaihtoehdon analyysi vahvistaa, että Euroopan tasolla toteutettavasta toiminnasta saataisiin lisäarvoa, minkä vuoksi se on todella tarpeen. Kolmas vaihtoehto näyttäisi tarjoavan eniten etuja.

Koska elintärkeiden infrastruktuurien suojaamista koskeva EU:n ohjelma on aivan uusi toiminta-ala, jolla toimia on tarpeen toteuttaa vaiheittain, käytännöllisin toimintamalli on kuitenkin toisen ja kolmannen vaihtoehdon yhdistelmä. Tämän vuoksi suojaamisohjelman yleiset puitteet perustuisivat periaatteisiin, joiden noudattaminen on vapaaehtoista, kun taas tietyt Euroopan elintärkeiden infrastruktuurien suojaamiseen liittyvät keskeiset vaatimukset täytettäisiin sitovien toimenpiteiden avulla.

Sitovista ja ei-sitovista toimenpiteistä muodostuvan suositellun toimintamallin vaikutukset

Jotta vähitellen voidaan ottaa käyttöön elintärkeiden infrastruktuurien suojaamista koskeva kattava ja johdonmukainen EU:n ohjelma, tarvitaan sekä sitovia että vapaaehtoisuuteen perustuvia toimenpiteitä.

Ohjelman jokaisen keskeisen osa-alueen toteuttamista varten arvioidaan sekä sitovien että vapaaehtoisuuteen perustuvien toimenpiteiden vaikutuksia[1]. Koska ohjelman yleisenä tavoitteena on parantaa elintärkeiden infrastruktuurien suojaamista Euroopan unionissa, keskeisten osa-alueiden turvallisuuden paranemista tarkastellaan suhteessa siitä aiheutuviin kustannuksiin.

1. *EU:n tason asiantuntijaryhmät.* Jotta elintärkeiden infrastruktuurien suojaaminen tuottaisi tuloksia pitkällä aikavälillä, on erittäin tärkeää rakentaa luottamusta kaikkien toimintaan osallistuvien sidosryhmien kesken. Asiantuntijaryhmät voivat edistää turvallisuuden lisääntymistä merkittävästi. Kustannukset ovat kohtuulliset, sillä asiantuntijaryhmiä perustettaisiin vain tarpeen mukaan ja ne toimisivat korvauksetta (*pro bono* -pohjalta). Koska EU:n tason asiantuntijaryhmien toiminta perustuisi vapaaehtoisuuteen, niiden tulisi olla osa suojaamisohjelman ei-sitovaa kehystä.

2. *Suojattu tietojenvaihto.* Elintärkeiden infrastruktuurien suojaamiseen liittyvien tietojen vaihto edellyttää sidosryhmien keskinäistä luottamusta. Vapaaehtoisuuteen perustuvaa tietojenvaihtoa ei voida tukea sitovin toimenpitein, koska ne eivät edistä luottamuksen rakentamista eivätkä helpota vuoropuhelua. Turvallisuutta tällainen tietojenvaihto toki lisäisi. Kustannukset jäisivät todennäköisesti vähäisiksi, koska toimenpiteet eivät ole sitovia, ja niiden tehtävänä olisi pikemminkin edistää tietynlaista turvallisuuskysymyksiin orientoitunutta ajattelutapaa.

3. *Keskinäisten riippuvuussuhteiden selvittäminen ja analysointi.* Sekä maantieteellisten että eri alojen keskinäisten riippuvuussuhteiden selvittäminen ja analysointi on Euroopan elintärkeiden infrastruktuurien suojaamisen parantamisen kannalta erittäin tärkeä tehtävä. Sitä varten ei voida ottaa käyttöön sitovia toimenpiteitä, sillä keskinäisten riippuvuussuhteiden selvittäminen on osa laajempaa prosessia, joka edellyttää eri sidosryhmien yhteistyötä ja toiminnan koordinointia. Kustannuksia on mahdotonta arvioida tässä vaiheessa, sillä keskinäisten riippuvuussuhteiden selvittäminen vaatii jatkuvaa työtä. Toimintaa voitaisiin tukea EU:n rahoituksen avulla.

4. *Kansalliset suojaamisohjelmat.* Vaikka vastuu kansallisten elintärkeiden infrastruktuurien suojelusta kuuluu selkeästi niiden omistajille/ylläpitäjille ja jäsenvaltioille, yhteisön kannalta olisi hyödyllistä varmistaa, että kansallisten elintärkeiden infrastruktuurien suojaamisesta on huolehdittu riittävästi kaikissa jäsenvaltioissa. Vaikka sitovasta velvollisuudesta laatia kansallinen suojaamisohjelma olisi turvallisuuden kannalta selkeää etua, tällaista velvollisuutta ei välttämättä voida säätää vielä tässä vaiheessa. Toissijaisuusperiaatteen ja EU:n tason suojaamisohjelman vaiheittaisen toteuttamisen vuoksi voi olla perusteltua keskittää sitovat toimenpiteet Euroopan elintärkeisiin infrastruktuureihin liittyviin kysymyksiin. Kansalliset suojaamisohjelmat saattaa olla perusteltua toteuttaa vapaaehtoispohjalta. Tätä ratkaisua on kuitenkin arvioitava uudelleen sen jälkeen kun Euroopan elintärkeiden infrastruktuurien määrittämisessä edistytään.

---

[1] Jotkin osa-alueet, kuten asiantuntijaryhmien perustaminen, voidaan toteuttaa vain vapaaehtoisuuteen perustuvin toimenpitein. Tällöin arvioinnissa käsitellään ainoastaan vapaaehtoisuuteen perustuvia toimia.

5. *Kansallisten elintärkeiden infrastruktuurien määrittäminen.* Jokaisen jäsenvaltion on määritettävä omat elintärkeät infrastruktuurinsa, jotta niitä voidaan suojata riittävällä tavalla. Tällaisen velvoitteen asettaminen toisi merkittävämpiä turvallisuusetuja kuin toiminnan toteuttaminen vapaaehtoiselta pohjalta. Toissijaisuusperiaatteen vuoksi ja siksi, että alkuvaiheessa on syytä keskittyä Euroopan tason elintärkeisiin infrastruktuureihin, saattaisi olla perusteltua määrittää kansallisen tason elintärkeät infrastruktuurit vapaaehtoispohjalta. Sitä mukaa kuin EU:ssa saadaan lisää kokemusta elintärkeiden infrastruktuurien suojaamisesta, toimintamallia saattaa kuitenkin olla tarpeen tarkistaa.

6. *Kansalliset yhteyspisteet.* Jokaisen jäsenvaltion on nimettävä yhteyspiste, joka vastaa elintärkeiden infrastruktuurien suojaamiseen liittyvistä kysymyksistä jäsenvaltiossa ja koordinoi tähän liittyviä toimia sekä jäsenvaltion sisällä että muiden jäsenvaltioiden, neuvoston ja komission kanssa. Vain sitova velvoite takaa, että kaikki jäsenvaltiot toteuttavat tätä varten tarvittavat toimet. Vapaaehtoisuuteen perustuvat toimetkin saattaisivat toki tuottaa tulosta, mutta niiden avulla ei voitaisi taata, että jokainen jäsenvaltio nimeää elintärkeiden infrastruktuurien suojaamisesta vastaavan yhteyspisteen. Sen vuoksi on aiheellista säätää sitovasta velvoitteesta.

7. *Euroopan elintärkeiden infrastruktuurien määrittäminen ja nimeäminen.* Suojaamisohjelman keskeinen osa-alue on Euroopan elintärkeiden infrastruktuurien määrittäminen ja nimeäminen, sillä infrastruktuurien suojaamista ei voida parantaa ennen kuin suojaamistoimien kohde on määritetty. Tämä työ on tehtävä koordinoidusti, ja se on mahdollista ainoastaan EU:n tasolla.

   Suojaamisohjelman tavoitteet voidaan saavuttaa riittävän suurella todennäköisyydellä vain jos näiden infrastruktuurien määrittäminen ja nimeäminen määritellään sitovaksi velvollisuudeksi. Tätä koskevaan sitovaan velvoitteeseen liittyy kaksi muutakin myönteistä seikkaa:

   - läpinäkyvyys: kun elintärkeiden infrastruktuurien määrittäminen ja nimeäminen tapahtuu osana oikeudellista prosessia, jota jäsenvaltiot ja mahdollisesti muutkin tahot valvovat, toiminta on mahdollisimman läpinäkyvää;

   - vertailtavuus: kun elintärkeät infrastruktuurit määritellään yhteisten menetelmien ja kriteerien avulla, ne ovat keskenään vertailukelpoisia, eikä niitä voida määrittää eri jäsenvaltioissa kovin erilaisin perustein.

   Jos käytettäisiin vapaaehtoisuuteen perustuvaa menettelyä, jouduttaisiin tilanteeseen, jossa vain tietyt EU:n kannalta merkittävät elintärkeät infrastruktuurit tulisivat määritetyiksi. On koko EU:n edun mukaista poistaa tällaiset heikkoudet.

8. *Euroopan elintärkeiden infrastruktuurien haavoittuvuuden sekä niihin liittyvien uhkien ja riskien arviointi.* Jokaisen jäsenvaltion olisi arvioitava sen kannalta merkityksellisiin Euroopan elintärkeisiin infrastruktuureihin liittyvät riskit ja uhkatekijät. Arvioiden avulla voitaisiin parantaa näiden infrastruktuurien suojaamista. Koska kyseessä on suojaamisen parantamisen kannalta erittäin merkittävä tehtävä, olisi perusteltua tehdä siitä sitova velvoite. Ellei varmisteta, että kaikki jäsenvaltiot laativat tarvittavat arvioinnit, Euroopan elintärkeiden infrastruktuurien omistajat/ylläpitäjät eivät saa riittävästi tietoa mahdollisista uhkista, eikä EU:n tasolla voida arvioida suojaamistoimissa olevia puutteita.

9. *Euroopan elintärkeisiin infrastruktuureihin liittyvät velvoitteet.* Jotta tavoite Euroopan elintärkeiden infrastruktuurien suojaamisen parantamisesta voidaan saavuttaa, olisi säädettävä, että näiden infrastruktuurien omistajien/ylläpitäjien on nimettävä turvallisuusyhteyshenkilö ja laadittava turvallisuussuunnitelma. Nämä kaksi velvollisuutta on perusteltua säätää sitoviksi, sillä muutoin ei elintärkeiden infrastruktuurien suojaamista voida toteuttaa johdonmukaisella tavalla koko EU:n tasolla. Jos toimet perustuisivat vapaaehtoisuuteen, vain osa elintärkeistä infrastruktuureista täyttäisi nämä vaatimukset. Mahdollisten kustannusten vastapainoksi turvallisuus lisääntyisi, mikä vahvistaisi vakautta, ennakoitavuutta ja kuluttajien luottamusta liiketoimintaympäristöön, ja tämä puolestaan lisäisi liiketoimintamahdollisuuksia ja investointeja.

Päätelmät

Edellä esitetty yhdeksän keskeisen toimenpiteen analyysi osoittaa, että elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman tavoitteet voitaisiin saavuttaa parhaiten yhdistämällä sitovia ja vapaaehtoisuuteen perustuvia toimia. Näin voidaan myös saavuttaa paras kustannus–hyötysuhde. Yhdeksästä keskeisestä toimenpiteestä viisi soveltuisi paremmin ei-sitovaan kehykseen ja neljän tulisi olla pakollisia:

(I) Ei-sitovat toimenpiteet:

a) EU:n tason asiantuntijaryhmät;

b) suojattu tietojenvaihto;

c) keskinäisten riippuvuussuhteiden selvittäminen ja analysointi;

d) kansalliset suojaamisohjelmat;

e) kansallisten elintärkeiden infrastruktuurien määrittäminen.

(II) Sitovat toimenpiteet:

a) kansallisten yhteyspisteiden nimeäminen;

b) Euroopan elintärkeiden infrastruktuurien määrittäminen ja nimeäminen;

c) Euroopan elintärkeisiin infrastruktuureihin liittyvien uhkien ja riskien arviointi;

d) turvallisuussuunnitelmien laatiminen ja turvallisuusyhteyshenkilöiden nimeäminen.

EU:n tason suojaamisohjelman perustamista varten suositellaan näin ollen toimintamallia, joka käsittää seuraavat osatekijät:

1. komission tiedonannossa esitettävä yleinen, ei-sitova kehys elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman perustamisesta;

2. Sitova väline (direktiivi), joka koskee nimenomaan Euroopan elintärkeitä infrastruktuureja. Direktiivissä esitetään yhteinen menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten ja yhteinen lähestymistapa niiden suojaamisen parantamistarpeen arviointia varten.

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 12.12.2006
SEK(2006) 1648

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

Åtföljande dokument till

Förslag till

RÅDETS DIREKTIV

om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

{KOM(2006) 787 slutlig}
{SEK(2006) 1654}

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Bakgrund

Europeiska unionens säkerhet och ekonomi liksom medborgarnas välfärd beror på vissa infrastrukturer och de tjänster som dessa tillhandahåller. Förstörelse eller driftstörningar som drabbar infrastruktur som erbjuder nyckeltjänster kan leda till dödsfall, förlust av egendom och ett sammanbrott för den europeiska allmänhetens förtroende och moraliska styrka.

Kritisk infrastruktur kan skadas, förstöras eller drabbas av driftsstörningar till följd av ett antal mänskliga och naturliga orsaker. Alla sådana driftsstörningar eller manipulationer som drabbar kritisk infrastruktur bör, i möjligaste mån, vara korta, exceptionella, hanterliga, geografiskt isolerade och i minsta möjliga mån innebära negativ påverkan på medlemsstaternas, deras medborgares och Europeiska unionens välfärd.

Vari ligger problemet?

Det problem som måste hanteras är sårbarheten i de kritiska infrastrukturerna i Europa och den därmed sammanhängande sårbarheten i de tjänster som tillhandahålls genom dessa. Det underliggande problemet är att skyddet för kritisk infrastruktur i vissa medlemsstater är lågt och därför potentiellt kan öka andra medlemsstaters sårbarhet.

Vem berörs?

Problemet berör teoretiskt samtliga Europeiska unionens invånare, företag, medlemsstaternas regeringar och myndigheter samt Europeiska unionen som helhet. Effekterna kan vara både direkta (t.ex. dödsfall p.g.a. av terrorattacker) och indirekta (t.ex. driftsstörningar som drabbar vissa tjänster till följd av problem som uppkommer med en viss infrastruktur).

Varför är behovet av åtgärder på EU-nivå så akut?

- Ett växande antal medlemsstater utarbetar för närvarande egna strategier för skydd av kritisk infrastruktur och väntar på att kommissionen skall lägga fram ett allmänt program för skydd av europeisk kritisk infrastruktur, så att de kan anpassa sig till den gemensamma EU-strategin. Förseningar i antagandet av ett gemensamt regelverk skulle öka risken för att medlemsstaterna utvecklar olika inkompatibla strategier för skydd av kritisk infrastruktur.

- Svaga länkar måste elimineras, i synnerhet när dessa kan leda till gränsöverskridande effekter. Målet måste vara att minimera risken för att en medlemsstats bristande skydd för infrastrukturen på det egna territoriet drabbar någon annan stat.

- Extrakostnader för företag som verkar i fler än en medlemsstat till följd av att olika säkerhetsåtgärder tillämpas måste minimeras.

- Viss infrastruktur blir mer och mer europeisk, vilket innebär att en rent nationell strategi är otillräcklig. Exempel på sådana strukturer är oljeledningar och kraftnät.

- En del av arbetet rörande de närmare detaljerna för hur kritisk infrastruktur i Europa kan skyddas på ett bättre sätt (särskilt när det gäller sådana frågor som identifiering av ömsesidiga beroendeförhållanden) kan rimligen förväntas ta lång tid. Detta arbete bör inledas snarast möjligt och grunda sig på ett gemensamt tillvägagångssätt.

- Överläggningar med berörda parter har pågått sedan 2004 och har omfattat tre seminarier om skydd av kritisk infrastruktur inom EU, antagandet en grönbok, två informella möten med kontaktpunkterna för frågor som rör skyddet av kritisk infrastruktur och talrika bilaterala möten med företrädare för myndigheter och den privata sektorn.

- Brotts- och terrorhoten minskar inte och det finns ett intresse för ett samarbete mellan medlemsstaterna och kommissionen, med alla synergieffekter som det ger, för att skydda sig mot sådana hot.

Mål

Det övergripande målet med den föreslagna politiken om skydd av kritisk infrastruktur är att förbättra skyddet av kritisk infrastruktur inom EU.

För- och nackdelar med de fyra tydliga politiska alternativen

Ett antal möjliga politiska alternativ för att uppnå ovannämnda mål har identifierats:

1. Att avstå ifrån att ta upp frågor om skydd av kritisk infrastruktur på EU-nivå. Med detta alternativ skulle inga övergripande åtgärder vidtas på europeisk nivå.

   Alternativet att ”inte ändra politisk inriktning” stärker inte skyddet av den kritiska infrastrukturen i Europa. Det medför emellertid nackdelar på grund av konkurrensproblem, ökade kostnader för företagen och bristande säkerhet. Detta alternativ har underkänts av alla medlemsstaterna, då dessa generellt ser ett behov av att ta sig an skyddet av kritisk infrastruktur ur ett europeiskt perspektiv.

2. Införande av ett frivilligt regelverk. Detta alternativ skulle innebära att ett frivilligt regelverk infördes, men medlemsstaterna skulle själva besluta om de ville tillämpa det eller ej.

   Alternativet med ett ”frivilligt regelverk” har den klara fördelen att det är ett regelverk som utformas för att bygga upp förtroendet bland samtliga berörda parter. Denna fördel kan emellertid inte uppväga de stora nackdelarna med detta alternativ, bl.a. stigande kostnader, konkurrensproblem och den förhöjda säkerhetsrisken. Ett centralt problem med detta alternativ är säkerhetsfrågan. Ett frivilligt regelverk kommer aldrig att kunna utgöra den bas som krävs för att få samtliga medlemsstater att vidta tillräckliga skyddsåtgärder för sin kritiska infrastruktur.

3. Införande av en ”lätt” lagstiftningsram. Med detta alternativ skulle ett antal bindande åtgärder vidtas på europeisk nivå. Medlemsstaterna skulle omfattas av vissa allmänna skyldigheter, men utbyte av bästa praxis, dialog och ett förtroendebyggande arbete på EU-nivå kommer att betonas.

   Alternativet med en lätt lagstiftningsram ger den bästa balansen mellan fördelar och nackdelar. Denna strategi skulle säkerställa konkurrensen, sänka kostnaderna för företag som verkar i fler än en medlemsstat och öka säkerheten i Europeiska unionen. Dessa tydliga fördelar skulle överväga de nackdelar som kostnaderna medför. En annan möjlig nackdel med alternativet är att det leder till ännu ett regelverk inom EU. I säkerhetens intresse förefaller denna strategi emellertid motiverad.

4. Fullständig harmonisering på EU-nivå. Detta alternativ skulle innebära åtgärder för fullständig harmonisering på EU-nivå i syfte att organisera frågor som rör skyddet av kritisk infrastruktur i medlemsstaterna och de skyddskrav som gäller ägarna eller operatörerna av kritisk infrastruktur.

   Alternativet ”fullständig harmonisering” medför flera klara för- och nackdelar. Det positiva är att EU:s kritiska infrastruktur skulle få ett starkt skydd. Det negativa är att det medför höga kostnader och att det skulle bli svårt att bygga upp förtroendet bland berörda parter. Slutligen har detta alternativ redan avvisats av medlemsstaterna som vill vidareutveckla det europeiska programmet för skydd av kritisk infrastruktur och komplettera befintliga landvinningar. Detta alternativ skulle gå stick i stäv med subsidiaritets- och proportionalitetsprinciperna och med största sannolikhet förkastas av medlemsstaterna.

Analysen av de fyra ovannämnda politiska alternativen bekräftar att åtgärder på europeisk nivå skulle ha ett mervärde och att de verkligen behövs. Alternativ 3 förefaller ge de största fördelarna.

Eftersom det europeiska programmet för skydd av kritisk infrastruktur medför en helt ny politik, och att det därför föreligger ett behov av en progressiv strategi på området skydd av kritisk infrastruktur, skulle emellertid en kombination av alternativ 2 och 3 vara den lösning som lättast kunde uppnås i praktiken. Den övergripande ramen för det europeiska programmet för skydd av kritisk infrastruktur skulle därmed regleras genom ett icke-bindande instrument medan ett fåtal nyckelkrav i fråga om europeisk kritisk infrastruktur skulle införas genom bindande åtgärder.

Konsekvenser av det rekommenderade politiska alternativet med bindande och icke-bindande åtgärder

Behovet av en övergripande och sammanhållen progressiv strategi för att inrätta det europeiska programmet för skydd av kritisk infrastruktur förutsätter en kombination av bindande och icke-bindande åtgärder.

Effekterna av bindande och icke-bindande instrument bedöms för vart och ett av nyckelelementen[1]. Eftersom det allmänna målet med det europeiska programmet för skydd av kritisk infrastruktur är att skydda kritisk infrastruktur i EU, vägs nyckelelementens positiva effekt mot de potentiella kostnaderna.

1. *Deltagande i expertgrupper på EU-nivå för skydd av kritisk infrastruktur.* Förtroendeskapande åtgärder bland alla berörda parter som deltar i processen för skydd av kritisk infrastruktur är helt avgörande för att arbetet skall vara framgångsrikt på lång sikt. Sådana expertgrupper för skydd av kritisk infrastruktur skulle ha en mycket positiv inverkan på säkerheten. Kostnaderna skulle begränsas, eftersom expertgrupperna endast skulle inrättas i mån av behov och arbeta utan särskild ersättning. Eftersom expertgrupperna på EU-nivå skulle fungera på frivillig grund, bör de omfattas av den icke-bindande ramen för det europeiska programmet för skydd av kritisk infrastruktur.

[1] Vissa element kan p.g.a. sin natur endast omfattas av icke-bindande åtgärder, exempelvis inrättandet av expertgrupper. I dessa fall kommer bedömningen att begränsas till de icke-bindande åtgärderna.

2. *En säker process för utbyte av information som rör skydd av kritisk infrastruktur*. Processen för utbyte av information som rör skydd av kritisk infrastruktur mellan berörda parter förutsätter ett förtroendefullt förhållande mellan dessa. Stöd till frivilligt utbyte av information om skydd av kritisk infrastruktur kan inte genomföras med bindande åtgärder, eftersom det inverkar menligt på arbetet med att bygga upp förtroende och underlätta dialog. Effekterna på säkerheten skulle naturligtvis vara positiva. Kostnaderna kan förväntas ligga på en låg nivå, eftersom åtgärderna förblir frivilliga och främst syftar till att skapa ett visst säkerhetstänkande.

3. *Kartläggning och analys av ömsesidiga beroendeförhållanden.* Kartläggning och analys av ömsesidiga beroendeförhållanden – såväl geografiskt som sektorsvis – kommer att vara ett viktigt inslag arbetet med att förbättra skyddet av den kritiska infrastrukturen inom EU. Det finns inga möjligheter att föreskriva bindande åtgärder i detta sammanhang, eftersom kartläggningen av beroendeförhållandena utgör en del av en större process som kräver samarbete och samordning mellan olika berörda parter. En kostnadsbedömning kan för närvarande inte göras, eftersom arbetet med kartläggning av beroendeförhållanden fortfarande pågår. EU-finansiering skulle kunna bidra till den processen.

4. *Utarbetande av nationella program för skydd av kritisk infrastruktur*. Samtidigt som det är klart att ansvaret för skyddet av nationell kritisk infrastruktur ligger hos ägarna eller operatörerna av den nationella kritiska infrastrukturen och medlemsstaterna, skulle det också ligga i gemenskapens intresse att frågan om nationell kritisk infrastruktur behandlas grundligt i var och en av medlemsstaterna. Även om en bindande strategi för nationella program för skydd av kritisk infrastruktur skulle innebära tydliga säkerhetsfördelar, är det inte säkert att en sådan strategi är möjlig i ett första steg. Subsidiariteten och behovet av en progressiv strategi i fråga om det europeiska programmet för skydd av kritisk infrastruktur skulle kunna motivera att bindande åtgärder koncentreras till frågan om europeisk kritisk infrastruktur. Strategin skulle emellertid behöva ses över när arbetet i fråga om europeisk kritisk infrastruktur väl kommit igång.

5. *Medlemsstaternas kartläggning av sin nationella kritiska infrastruktur*. Kartläggningen av den nationella kritiska infrastrukturen är en förutsättning för att garantera att den skyddas på ett lämpligt sätt. Bindande åtgärder i samband med kartläggningen av nationell kritisk infrastruktur skulle ge tydligare säkerhetsfördelar än icke-bindande. På grund av subsidiariteten och behovet av att i första hand koncentrera sig på frågor som rör kritisk infrastruktur, kan emellertid en icke-bindande strategi för kartläggning av nationell kritisk infrastruktur motiveras. I takt med att EU:s erfarenhet i fråga om skydd av kritisk infrastruktur växer, kan denna strategi emellertid komma att omprövas.

6. *Varje medlemsstat utser en kontaktpunkt för skydd av kritisk infrastruktur*. Varje medlemsstat måste utse en kontaktpunkt för skydd av kritisk infrastruktur, vilken skulle kunna skaffa sig en allmän överblick över arbetet med skydd av kritisk infrastruktur i medlemsstaterna och samordningen av skyddet av kritisk infrastruktur inom medlemsstaterna samt med övriga medlemsstater, rådet och kommissionen. Endast bindande åtgärder skulle ge garantier för att de enskilda medlemsstaterna vidtar nödvändiga åtgärder. Icke-bindande åtgärder skulle kunna ha viss framgång, men inte på något sätt garantera att de enskilda medlemsstaterna verkligen utser en

kontaktpunkt för skydd av kritisk infrastruktur. Bäst vore därför en bindande strategi för hur kontaktpunkterna för skydd av kritisk infrastruktur utses.

7. *Kartläggning och definiering av europeisk kritisk infrastruktur.* Kartläggning och definiering av europeisk kritisk infrastruktur är ett centralt inslag i det europeiska programmet för skydd av kritisk infrastruktur, eftersom ett förbättrat skydd av kritisk infrastruktur kan bli verklighet först när relevant infrastruktur har kartlagts. Denna process måste slutföras på ett samordnat sätt och kan endast bli framgångsrik om den sker på EU-nivå.

   Endast en bindande strategi för kartläggning och definiering av europeisk kritisk infrastruktur kan med verklig sannolikhet leda till att målen med det europeiska programmet för skydd av kritisk infrastruktur uppfylls på ett framgångsrikt sätt. En bindande strategi i detta avseende skulle dessutom ha ytterligare två positiva effekter:

   - Öppenhet – om kartläggningen och definieringen är föremål för ett rättsligt förfarande innebär detta också en granskning från medlemsstaternas sida – och potentiellt från andra organ, varigenom öppenheten maximeras.

   - Jämförbarhet – garantier för gemensamma förfaranden och metoder innebär att de europeiska kritiska infrastrukturer som kartlagts kan jämföras och att medlemsstaterna inte behöver mötas av potentiellt mycket svåra tolkningsproblem.

   Om en icke-bindande strategi skulle tillämpas i denna process, skulle EU ställas inför en situation där endast viss europeisk kritisk infrastruktur som är av vikt för EU skulle kartläggas. Det ligger i hela EU:s intresse att undanröja sådana svaga länkar.

8. *Sårbarhets-, hot och riskbedömningar för europeiska programmet för skydd av kritisk infrastruktur*. Varje enskild medlemsstat bör genomföra en risk- och hotbedömning i förhållande till relevant europeisk kritisk infrastruktur. Sådana bedömningar skulle göras för att förbättra skyddet av europeisk kritisk infrastruktur. På grund av bedömningens roll i hela processen för att stärka skyddet av europeisk kritisk infrastruktur vore det i detta avseende motiverat att tillämpa ett bindande instrument. Om det inte säkerställdes att samtliga medlemsstater genomför lämpliga bedömningar, skulle ägarna eller operatörerna av europeisk kritisk infrastruktur inte förfoga över tillräcklig information om potentiella hot och en bedömning på EU-nivå av brister i skyddet skulle inte genomföras.

9. *Skyldigheter med avseende på europeisk kritisk infrastruktur*. För att uppnå målet att förbättra skyddet av europeisk kritisk infrastruktur, bör två åtgärder som kan utföras av ägare eller operatörer av europeisk kritisk infrastruktur övervägas: det bör utses en sambandsansvarig i säkerhetsfrågor och en säkerhetsplan bör utarbetas. Att tillämpa ett bindande instrument på dessa båda skyldigheter är motiverat, eftersom det vore omöjligt att nå fram till en gemensam strategi för skydd av europeisk kritisk infrastruktur inom hela EU på något annat sätt. Om icke-bindande åtgärder skulle tillämpas, skulle de endast genomföras inom ett begränsat antal europeiska kritiska infrastrukturer. Eventuella kostnader skulle åtminstone kunna uppvägas av förhöjd säkerhet, vilket innebär mer stabilitet, förutsägbarhet och en ökning av konsumenternas förtroende för företagen. Detta leder i sin tur till en bättre möjligheter för företagen och tilltagande investeringsvilja.

Slutsats

Analysen av den särskilda effekten av nio nyckelåtgärder och visar att en kombination av bindande och icke-bindande åtgärder vore den bästa vägen att uppnå målen för det europeiska programmet för skydd av kritisk infrastruktur, samtidigt som det är det mest kostnadseffektiva alternativet. Vad gäller de nio nyckelåtgärderna, skulle fem av dem fungera bäst om de vore icke-bindande, medan fyra bör göras bindande:

(I) Icke-bindande åtgärder:

a) att delta i expertgrupperna för skydd av infrastruktur på EU-nivå.

b) att tillämpa en process för utbyte av information om skydd av kritisk infrastruktur.

c) att kartlägga och analysera beroendeförhållanden.

d) att utarbeta nationella program för skydd av kritisk infrastruktur.

e) att kartlägga nationell kritisk infrastruktur.

(II) Bindande åtgärder:

a) att utse kontaktpunkter för skydd av kritisk infrastruktur.

b) att kartlägga och definiera europeisk kritisk infrastruktur.

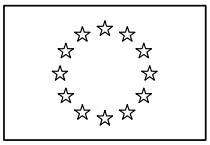
c) att genomföra hot- och riskbedömningar avseende europeisk kritisk infrastruktur.

d) att utarbeta säkerhetsplaner och utse sambandsansvariga för säkerhetsfrågor.

Därför bör den föreslagna politiken för inrättande av det europeiska programmet för skydd av kritisk infrastruktur omfatta följande:

1. En generell icke-bindande ram för ett europeiskt program för skydd av kritisk infrastruktur som fastställs i ett meddelande från kommissionen.

2. Ett bindande instrument som särskilt avser europeisk kritisk infrastruktur (direktivet om europeisk kritisk infrastruktur). Detta instrument skulle föreskriva en gemensam strategi för att kartlägga och definiera europeisk kritisk infrastruktur för att kunna bedöma behovet av att förbättra skyddet av denna infrastruktur.



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2006
SEC(2006) 1654

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

COUNCIL DIRECTIVE

on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

IMPACT ASSESSMENT

{COM(2006) 787 final}
{SEC(2006) 1648}

Table of contents

Impact assessment

The European Programme for Critical Infrastructure Protection

Executive summary

The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU.

Critical infrastructure can be damaged, destroyed or disrupted through a variety of both manmade and natural occurrences. Any such disruptions or manipulations of critical infrastructure should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

In order to counteract these potential vulnerabilities the Commission was requested by the European Council in 2004 to present a European Programme for Critical Infrastructure Protection. Since then, intensive preparatory work has been undertaken, which has included the organisation of relevant seminars, the publication of a Green Paper and discussions with stakeholders.

The general objective of a proposed policy on critical infrastructure protection would be to improve the protection of critical infrastructure in the EU. A number of possible policy options have been identified with a view to achieving this objective:

1. Refraining from addressing CIP issues at a European level.
2. The creation of a non-binding framework.
3. The creation of a light legislative framework.
4. Full harmonization at EU level.

Following a careful analysis and due to the broad scope of the envisaged policy and the need for a step-by-step approach to CIP, it appeared that setting up EPCIP by a non-binding instrument such as a Communication, complemented by a restricted number of binding measures, offers the best cost/benefit ratio and best satisfies the underlying objective of improving the protection of critical infrastructure in Europe and thereby increasing the security of the European Union and its citizens.

Section 1: Procedural issues and consultation of interested parties

Organisation and timing

Reference number: 2006/JLS/045

Work on the European Programme on Critical Infrastructure Protection began in 2004 following the terrorist attacks in Madrid. Relevant work has been taken forward through the Critical Infrastructure Protection sub-group of the Interservice Group on the Internal Aspects of the Fight Against Terrorism. This CIP sub-group is chaired by DG JLS with participation from: DG TREN, DG MARKT, DG INFSO, DG ADMIN, DG ECFIN, DG ENTR, DG SANCO, DG RTD, DG ENV, JRC, DG REGIO, DG RELEX, DG BUDG, OLAF, SJ and SG.

Consultation and expertise

All relevant stakeholders have been consulted concerning the development of EPCIP. This has been done through:

- The EPCIP Green Paper adopted in on 17 November 2005 with the consultation period ending on 15 January 2006. 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments to the Green Paper. The responses were generally supportive of the idea of creating EPCIP. Summary reports concerning the responses received from the Member States and the private sector to the EPCIP Green Paper consultation are included in Annex 1 and 2.
- Three Critical Infrastructure Protection seminars hosted by the Commission (in June 2005, September 2005 and March 2006). All three seminars brought together representatives of the Member States. The private sector was invited to the seminars held in September 2005 and March 2006.
- Informal meetings of CIP Contact Points. The Commission hosted two meetings of the CIP Contact Points of the Member States (December 2005 and February 2006).
- Informal meetings with private sector representatives. Numerous informal meetings were held with representatives of particular private business as well as with industry associations.

Impact of the Green Paper responses on the EPCIP proposal

As a result of the responses received to the EPCIP Green Paper and of ongoing discussions with all stakeholders, the following issues have had a major impact in shaping the proposal for EPCIP:

- *Goal of EPCIP*. The goal of EPCIP has been changed to improving the protection of critical infrastructure in the EU. Previously, the proposed goal of EPCIP was to ensure that there are adequate and equal levels of protective security on critical infrastructure. Several stakeholders underlined in their responses to the EPCIP Green Paper that the setting of equal levels of protective security across all sectors would not only be extremely difficult to achieve, but could also be counterproductive in terms of increasing security overall as sector specificities would not be taken into account sufficiently.
- *Key principles.* The list of key principles has been expanded to include the "sector-by-sector approach". The remaining principles have also been modified.
- *Common EPCIP framework.* It is explicitly acknowledged that the common EPCIP framework must be of a general nature and should contain only the most important

provisions needed to facilitate future work. Specific work along with further regulatory activities (where relevant) will be taken forward on a sectoral basis.

- *ECI and NCI.* The approach to ECI and NCI has been clearly separated, by introducing a common approach to ECI at EU level and leaving the introduction of similar approaches for NCI to the Member States, where necessary supported by the Commission. .
- *Implementing steps for ECI and NCI.* The implementing steps have been amended in order to take account of the varying role the EU may play in relation to ECI as compared to NCI. A structured system of implementation has been proposed consisting of three Work Streams (the first of a strategic/horizontal nature, the second concerning ECI, the third concerning NCI).
- *Single overseeing body.* The Member States remain free to establish administrative structures as they see fit in order to deal with CIP. EPCIP would only require that each Member State designate a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission.
- *National CIP Programmes.* EPCIP would only encourage each Member State to develop a National CIP Programme based on a certain set of recommended elements.
- *Identification of NCI.* It has been clarified that the identification of NCI would remain in the hands of the Member States.
- *Identification of ECI.* A set of procedures for the identification and designation of ECI has been put forward.
- *Owners/operators of critical infrastructure.* Their obligations and rights have been clarified.
- *Confidentiality and information exchange.* Due to the very big importance attributed to this issue by stakeholders, confidentiality and the exchange of CIP related information has been specifically address.

Section 2: Problem definition

What is the issue or problem that may require action?

The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The existence and operation of for example - telecommunication and energy networks, banking and transport systems, health services, the provision of safe drinking water and food - is crucial to the functioning of the European Union and its Member States. The destruction or disruption of infrastructure providing key services could entail *inter alia* the loss of lives, the loss of property, a collapse of public confidence and moral in the EU.

Critical infrastructure can be damaged, destroyed or disrupted in a multitude of ways including deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. Any such disruptions or manipulations of critical infrastructure should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States (MS), their citizens and the European Union. The recent terrorist attacks in Madrid and London have highlighted the risk of terrorist attacks against infrastructure in Europe.

The critical infrastructure present in the European Union is currently subjected to a varying puzzle of protective measures and obligations. Some Member States have already identified their national critical infrastructure and have imposed strong protection measures. Several other Member States are not as advanced however. In certain cases, there has been no concerted effort to even identify the critical infrastructure present under a particular jurisdiction.

Despite the fact that some work has been undertaken at national level in order to deal with national critical infrastructure, very little has been done in terms of studying the interdependencies existing between critical infrastructure in various sectors as well as the interdependencies existing between infrastructure located in different Member States. No effort has been done to identify those critical infrastructures which if disrupted or destroyed could have a significant effect on the functioning of the Community as a whole or a number of Member States. It is clear however that such critical infrastructure exist.

The damage or loss of a piece of infrastructure in one MS may have negative effects on several others and on the European economy as a whole. This is becoming increasingly likely as new technologies (e.g. the Internet) and market liberalisation (e.g. in electricity and gas supply) mean that much infrastructure is part of a larger network.

It is clear, that the security of critical infrastructure is only as strong as its weakest link. In other words, even if one Member States imposes very high security standards in relation to a particular cross-border infrastructure, that infrastructure and the services it provides will still be vulnerable if another Member State does not impose adequate protection measures on its side.

It is also evident that in today's interconnected world, infrastructure physically located in a single Member State may offer services to other Member States or may have an impact on the provision of services in other Member States. In the case of such infrastructure, it is equally important to provide this particular infrastructure with a sufficient level of security so that the security of other Member States, who are dependent on the service that infrastructure provides or may be influenced by that infrastructure, is ensured. The interdependencies existing between the various sectors create a situation where a particular event may have a cascading effect on other sectors

and areas of life, which are not immediately and obviously interconnected. For example, a terrorist attack on a power plant may disrupt the power supplies over a large area and may influence the provision of other services including medical services due to the lack of electricity. Interdependencies exist within and between businesses, industry sectors, geographical jurisdictions and MS authorities in particular those enabled by Information and Communications Technologies (ICTs).

Many European companies operate across borders and as such are subject to differing obligations concerning critical infrastructure. On the purely economic side, the existence of a multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur duplicating security investments depending on the jurisdictions under which they operate.

The underlying problem is that a low level of protection of critical infrastructure in certain Member States has the potential to increase the vulnerability of other Member States. The basic principle of coexistence or sharing of a common space implies however that no co-owner of that common space should allow that any harm be caused, deliberately or not, to their neighbours.

The problem in general

The issue at hand which requires action is the vulnerability of critical infrastructures in Europe and the ensuing vulnerability of the services they provide. This applies to all critical infrastructures in Europe regardless of whether they can be considered as having EU or national importance.

Taking into account the principles of subsidiarity and proportionality, EU level action should concentrate on those critical infrastructures having an EU importance. With this in mind, EPCIP will develop into a process leading over time to an assessment of vulnerabilities of particular CI sectors and the preparation of proposals on how to best address these vulnerabilities. These key activities and especially the development of specific protection measures will concentrate on European critical infrastructure, with the Member States however being encouraged to adopt similar approaches concerning their national critical infrastructure.

What are the underlying drivers of the problem?

The vulnerability of critical infrastructure in the European Union is caused by:

- Certain owners/operators of critical infrastructure may not be implementing sufficient protection measures (possibly because they are not aware of potential risks or they do not want to over-invest is security and put themselves in a competitive disadvantage vis-à-vis other businesses)
- Certain Member States do not possess detailed and systemised knowledge about the existence of critical infrastructure under their jurisdiction.
- Certain Member States have not established a national approach to strengthening the protection of critical infrastructure under their jurisdiction
- No systematic effort has been made to identify interdependencies existing between sectors and between critical infrastructure existing in various Member States.

Who is affected, in what ways, and to what extent?

The problem potentially affects all European citizens, inhabitants of the European Union, the Member State governments and the European Union as a whole. Effects can be both direct (e.g. casualties following a terrorist attack) and indirect (e.g. the disruption of certain services following the surfacing of problems with a particular infrastructure).

- *Citizens.* The existence of vulnerable infrastructure affects EU citizens by way of the potential loss of lives, the destruction of private property and the disruption of services.
- *Business.* The existence of vulnerable infrastructure affects EU businesses by way of the potential destruction of property and the disruption of services/shipments businesses rely on. EU businesses are very much interdependent (both geographically and in terms of sectors), so a disruption/destruction of a single critical infrastructure may have detrimental effects on a number of associated businesses. It is moreover worth mentioning, that competition among businesses creates a situation in which businesses are less likely to invest in sufficient security if their competitors aren't investing either.
- *Governments.* Governments are affected by the existence of vulnerable infrastructure as they too are dependent on services provided by such infrastructure. The potential disruption/destruction of critical infrastructure may wane public confidence in acting governments.

The costs for owners/operators of critical infrastructure should a disruption or destruction of infrastructure occur

Risks to critical infrastructure industries are becoming more and more interdependent as the economic, technological, and social processes of globalization intensify. The challenge of ensuring reliable operations has increased because operations both within and among companies have become increasingly interdependent. Elements of infrastructure in particular have become so interdependent that the destabilization of one is likely to have severe consequences for others.

As the scale and reach of technological systems have increased, the potential economic and social damage of failures has increased as well. The sources of such major disruptions lie in technical and managerial failures as well as natural disasters or terrorist attacks. Economic and social activities are becoming more and more interdependent as well, so that the actions taken by one organization will affect others.

In this context, the incentives for any single organization to invest in prevention, response, and recovery are blunted. Without an EU approach to understanding interdependencies and security externalities, determining the source of disruptions and quantifying the risk of such disruptions are difficult. Private decision-makers will have neither adequate information nor adequate motivation to undertake investments that are more than justifiable from the standpoint of the system as a whole.

Strategies to protect critical infrastructure are not viable unless they are politically and economically sustainable. Sustainability may be enhanced by a deliberate policy of seeking win-win options that promise public and private benefits beyond vulnerability reduction. Public relations, reputation, and the possibility of tort liability may motivate some firms to invest.

Understanding the motives, constraints, and capabilities of potential attackers may inform decisions regarding investments in prevention, response, and recovery.

A market economy routinely accounts for improved efficiency, because shareholders are always looking for the best return on investment in the short term. However, vulnerability may be assessed only after it has been exposed by active study or system failure. In addition, organizations are most likely to account for vulnerabilities that are linked to their own core activities.

Accountability for and accounting of vulnerabilities distant from core business activities are relatively uncommon, particularly when the perceived probabilities of occurrence are very low. Although economic incentives drive the accounting of core-business vulnerabilities, legal, organizational, and political dynamics drive the response to vulnerabilities that lie outside the core business concerns of any single firm or industry.

The cumulative impact of terrorist attacks and natural disasters has raised the bar on corporate governance. Owners/operators are increasingly under heightened scrutiny to identify vulnerabilities and prepare flexible disaster recovery plans to protect corporate as well as personal assets as well as prepare for, and manage catastrophic emergencies that can have a crippling effect on their business.

Protecting employees, revenue, and assets are all components of a well thought out plan aimed at minimizing loss and liability. A critical infrastructure owner/operator's failure to identify its exposures and evaluate the impact of potential losses could be disruptive to the continuity of its business leaving its executives open to severe legal actions and public criticism. While owners/operators of critical infrastructure may have good reasons not to make public disclosures regarding security breaches, one would expect their incentives to measure the costs of such incidents internally to be strong.

Without accurate cost data (how would critical infrastructure owners/operators assess the risks they face, make rational decisions about how much to spend on information security, or evaluate the effectiveness of security efforts etc.) it is very difficult to quantify the costs ensuing from potential terrorist attacks, natural disasters or other major occurrences. These costs will depend on the sector in which the disrupted/destroyed infrastructure operates, its size, interdependencies etc. What we can be sure of is that depending on the nature of the threat, a number of direct and indirect costs will affect not only the entity which was the object of the attack/occurrence, but also its business partners, employees and the wider public.

Given the uncertainties in measuring costs, risks, and the effectiveness of security efforts, we cannot make simple statements like the following: a company that expects to lose x euros per year to cyber attacks, natural disasters or terrorism will generally spend y euros to mitigate those losses.

In the case of a terrorist attack against a particular infrastructure asset, the relevant costs could be incurred in five areas:

1. The owners/operators that were the target of the attack. Direct impacts would include casualties, physical damage, and loss of production capacity. Indirect consequences could include the resignation of staff, loss of business.

2. Other actors located in the physical proximity of the target. Direct impacts could include casualties and physical damage. Indirect consequences could include resignation of staff and the loss of business.
3. Associated actors. Costs would be incurred for example by the business partners of the targeted owners/operators who would no longer be able to supply a specific product or service.
4. All other actors including the broader public. This will entail a fall in business and consumer confidence.
5. The cost will also be related to the government's emergency response and reconstruction efforts

The macroeconomic costs stemming from a terrorist attack continue to grow as businesses become more interdependent. Unfortunately, terrorist attacks themselves are increasingly inexpensive to conduct. To illustrate the disproportions existing between these costs, it is worth recalling the costs of carrying out some recent terrorist attacks.

The November 1998 twin truck bombings of the U.S. embassies in Kenya and Tanzania was estimated to cost less than $50,000. The September 11, 2001 attack cost an estimated $500,000. 231 people died in the two embassy bombings while almost 3,000 died during September 11, 2001. The cost of reconstruction of the U.S. embassies was a fraction of the $2 trillion estimated reconstruction cost and losses caused by Sept. 11, 2001.

The cost of the terrorist attack in Istanbul in November 2003 was estimated at less than $40,000. Four suicide truck bombings hit four different targets, killing 62 people. The attack reversed the country's slow economic recovery and caused a capital outflow by Western investors.

The Madrid bombings killed 191 people and cost as little as $10,000. The London and Sharm el Sheikh attacks in 2005 killed 55 and 88 people respectively and cost roughly the same or less, yet their potential socio-economic impact (potential cost of lost business, reconstruction, insurance and security) is much higher. In the case of the London and Madrid bombings, the reduction to the Spanish and UK's gross domestic product appears to have been negligible.

Effective action to combat terrorism will generate significant benefits for the global economy, preventing losses from reduced trade flows and investment undermining economic growth. Since international goods and financial markets transmit terrorism's costs well beyond the country where acts occur and terrorist groups operate across borders, any economy's actions to curb terrorist activities should produce global and regional benefits. Similarly, failure to counter terrorism will produce costs for all economies and populations. When consumers feel less safe, it changes their spending patterns. Businesses will change their investment and employment plans. Lack of confidence negatively impacts growth.

A sustainable critical infrastructure policy must account for tradeoffs that exist not only at company level between efficiency and vulnerability but also for institutions and the incentives potentially affecting that trade-off. Ultimately, policy must

- structure incentive systems for investment that enhance prevention of, response to, and recovery from the most likely and damaging attacks;

- ensure adequately robust internal operations of private firms, including greater system reliability for their services;
- limit imposed costs on firms to guarantee the competitiveness of the economy; and
- do all of the above in a manner that can be sustained by a public with a short memory that may tire of the high costs and consumer inconvenience that policies aimed at making critical industries less vulnerable may entail.

Cost is a significant issue when considering security of critical infrastructure in the EU. A lot of money is already spent by government agencies (e.g. police, border guards) and by commercial organisations (e.g. for security of premises). Increasing the security against terrorism will cost even more money. However budgets of both governments and commercial organisations are getting increasingly tight, and money for new security measures will be hard to find. In some ways, cost is a key driver and may be more significant than technology in terms of the level of security that can be provided within the EU[1].

Security costs money in two basic ways: cost of security equipment and cost of security staff. Some security equipment can save in staff costs. For example, automatic processing of CCTV images can reduce the number of staff required to monitor CCTV, thus saving on staff costs, while at the same time increasing security effectiveness. However, most new security equipment and procedures to increase effectiveness will require increased spending on security.

There are some significant differences between the costing philosophy for measures to fight *crime* (i.e. criminal acts for monetary gain) and for measures to fight *terrorism* (i.e. criminal acts to cause destruction and fear). Acts of crime are much more frequent than acts of terrorism, and counter crime measures effectively pay for themselves in terms of reduced financial losses. In fact commercial organisations may allow a measure of loss due to fraud or theft because measures to give 100% protection against fraud or theft are seen as not cost effective.

The problem with security against terrorism is that if an attack does not happen, the money could be regarded as having been wasted – although it could be instead be regarded as a form of insurance. However, if the same measures could protect both against terrorism and against more conventional crime, then the savings against crime will effectively pay (wholly or partially) for the security.

Some security costs can effectively be paid for by the end user by legislation which requires the service providers (e.g. transport company, utility) to provide a certain level of security. Thus, for example:

a) Transport security may be paid for by the traveller through increased fares
b) Goods security may be paid for by the sender/receiver through increased freight charges
c) Energy/telecoms/water security may be paid for by the customer through higher bills
d) Computer and data network security may be paid for by the customer through increased hardware/software costs, higher charges for sending data and higher rentals for connections/services.

[1] ESSRT Project funded by the European Commission under the PASR 2004 Programme (Thales Research and Technology; International Institute for Strategic Studies; Crisis Management Initiative; Thales e-Security).

If the cost increase due to extra security is below the rate of inflation, it might be easier to get it accepted. However, security legislation and consequent cost increases might push some business away from the EU to less security conscious nations.

Some security costs will have to be paid for out of taxation, e.g. border surveillance, law enforcement staff, armed response units on standby, security of government buildings and networks.

The difficulty with the economics of protection against terrorism is that there is no way of being fully sure that security measures are going to be effective. Millions of Euros might be spent on advanced security measures and an attack with very costly consequences still happens. It will be difficult to know if the security measures adopted had any real effect. Some clues might be given if an attack about to happen was prevented by the security measures. However it will be virtually impossible to quantify the deterrent effect of any security measures, i.e. whether terrorists would have tried an attack if those measures were not in place.

Another thing to consider is the difficulty of calculating the cost of national security -- and in particular of identifying the part of security costs that may be said to be counter-terrorism. A nation's security is paid for partly out of the defence budget, for which a global figure is usually given, but in most countries is very hard to break this down into its component parts. However, security is also paid for out of a range of other budgets: those of interior ministries, transport ministries, justice ministries, intelligence agencies, co-ordinating bodies, health service, local government bodies of all kinds, as well as private companies and individuals. This makes it virtually impossible to quantify security costs for each country, and to compare one country with another. For example, what proportion of a policeman's salary is attributed to national security/counter-terrorism?

An example of an indicative assessment of who is likely to pay for individual security measures directly and indirectly can be outlined as follows. This data is provided purely as an example of what types of security measures may be needed in order to improve the protection of critical infrastructure in Europe and the potential costs involved. Detailed impact assessments will accompany proposals for specific protection measures on a CIP sector-by-sector basis which may be developed where relevant. Cost issues will limit what can be achieved on European security, and spending must be prioritised wisely according to probability and impact of potential threats.

Security solution	Paid for by
Person access control Person scanning Luggage scanning	1. Boarding transport (e.g. aircraft, train) – *Paid for by transport companies and passed on within transport fares* 2. Crossing border – *Paid for within transport companies and passed on within transport fares (air/sea border), or by government from taxation (land border)* 3. Entering protected building or site – *Paid for by building/site user*
Vehicle access control Goods integrity control Vehicle/ container/ goods scanning	1. Boarding ship/train – *Paid for by transport companies and passed on within transport charges* *2.* Crossing air/sea border - *Paid for within transport companies and passed on within transport fares* 3. Crossing land border *Paid for by government from taxation* 4. Entering protected building or site – *Paid for by building/site user, but passed on to customers by users who are commercial organisations*
Perimeter protection	*Paid for by building/site user, but passed on to customers by users who are commercial organisations*
Land border surveillance	*Paid for by government from taxation*
Remote surveillance	1. Public area – *Paid for by area user, but passed on to customers by users who are commercial organisations* *2.* Public roads - *Paid for by government from taxation* 3. Other transport network – *Paid for by transport companies and passed on within transport charges* 4. Energy supply network – *Paid for by energy users*
Water quality checking	*Paid for by water companies and passed on in water charges*
General intelligence	*Paid for by government from taxation*
Ship and port protection	*Paid for within shipping and port companies/authorities and passed on within transport charges*
Maritime border protection	*Paid for by government from taxation*
Airspace protection	*Paid for by government from taxation*
CBR release detection	1. Public areas - *Paid for by users of the area, but passed on to customers by users who are commercial organisations* 2. Public events – *Paid for by government but passed on to event organisers and thence to event attendees*
EMP protection	1. Equipment - *Paid for in equipment costs* 2. Networks – *Paid for by network owners but passed on to customers*
Data and data network protection	*1.* Equipment and network within an organisation/agency - *Paid for by that organisation/agency* 2. Network between organisations/agencies – *Paid for by arrangement between the organisations/agencies served*

How would the problem evolve, all things being equal?

The problem would evolve taking into account the following:

- Member States would continue to address CIP issues individually
- A certain number of sectoral initiatives would appear at European level

If the problem would continue evolving without horizontal actions at EU level, no broader CIP coordination would exist. Consequently, there would be a strong risk that various incompatible sectoral approaches would be developed.

At national level, the EU Member States would continue to address CIP issues at their own pace. Certain Member States would continue to strengthen their CIP initiatives, while others would not pay much attention to the issue assessing their potential risk as low. Differences in protection measures among the Member States would mean that, especially for certain interdependent infrastructure, vulnerability would be quite high.

Businesses would refrain from investing in security issues as the existence of a multitude of standards and obligations would decrease their competitiveness.

Ultimately, the security of European citizens would suffer as a result.

Does the EU have the right to act?

Although several sectoral legal bases for critical infrastructure protection exist (e.g. in the transport and energy sectors), the Treaty does not specifically address CIP issues in a horizontal fashion. The Treaty establishing the European Community identifies nevertheless in Article 2 a number of objectives, whose attainment could be facilitated by strengthening the protection of critical infrastructure in Europe:

- To promote a harmonious, balanced and sustainable development of economic activities
- To promote a high degree of competitiveness
- To promote a high level of protection and improvement of the quality of the environment
- To promote the raising of the standard of living and quality of life
- To promote solidarity among Member States.

An EU policy on critical infrastructure protection would have to involve a number of sectors (in which varying forms of Community competence exist). Moreover, each of these sectors would have to deal with critical infrastructure protection by way of an all-hazards approach (involving both manmade and natural threats).

At present no act of the Community deals with the establishment or security aspects of a common framework for critical infrastructure protection in the EU.

The EU right to act has been acknowledged by the Council, which requested the Commission, to develop a programme to improve the protection of critical infrastructure in Europe.

The European Council of June 2004 asked for the preparation of an overall strategy to protect critical infrastructure. In response, the Commission adopted on 20 October 2004 a Communication "Critical Infrastructure Protection in the Fight Against Terrorism" putting forward clear suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructure.

The Council conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the set-up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN).

The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection by June 2006. The Conclusions state that "(…) the Council considers that action at EU level will add value by supporting and complementing Member States' activities, while respecting the principle of subsidiarity".

The subsidiarity principle is satisfied as the measures being undertaken through this proposal cannot be achieved by any single EU Member State and must therefore be addressed at EU level. Although it is the responsibility of each Member State to protect the critical infrastructure present under its jurisdiction, it is crucial for the security of the European Union to make sure that the most important infrastructure having an impact on two or more Member States or on a single Member State if the critical infrastructure is situated in another Member State are protected to a satisfying degree and that particular Member States are not made vulnerable because of the existence of lower security standards in other Member States.

Why is EU level action urgently needed?

- A growing number of Member States are preparing their own approaches to critical infrastructure protection and are waiting for the Commission to put forward a general European CIP programme, so that they can take into account the common EU approach. Delaying the adoption of a common framework would increase the chance that various incompatible approaches to CIP would be developed by the Member States.
- Weak links have to be eliminated especially where transboundary effects came into play. The risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory needs to be minimised.
- Additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimised.
- Some infrastructure are becoming increasingly European, which means that a purely national approach is insufficient e.g. the energy pipelines and transmission network.
- Some of the work concerning the details of how to better protection critical infrastructure in Europe (especially on such issues as the identification of interdependencies) can reasonably be expected to take a long time. Such work should start as quickly as possible and needs to be based on a common approach.
- Stakeholder consultations have been ongoing since 2004 and have included three EU CIP Seminars, the adoption of a Green Paper, the holding of two informal CIP contact points meetings and numerous bilateral meetings with government and private sector representatives.
- Criminal and terrorist threats are not diminishing and that there is an interest, and potentially synergies, in Member States and the Commission cooperating to protect against them.

Section 3: Objectives

The general objective of the proposed policy would be to improve the protection of critical infrastructure in the EU.

The specific and operational objectives needed in order for the general objective to be achieved are:

- Ensure that owners/operators of critical infrastructure implement adequate protection measures
    - Make sure that owners/operators of European Critical Infrastructure conduct sufficient risk assessments and prepare operator security plans
    - Make sure that owners/operators have access to best practices in the field of CIP
    - Ensure that all owners/operators of European Critical Infrastructure are subject to similar general requirements concerning critical infrastructure protection. These general requirements would not address the issue of specific protection measures, but would rather introduce a common approach on the steps to be taken and issues to be addressed by the owners/operators in order to improve the security of European critical infrastructure.
    - Ensure that owners/operators of European Critical Infrastructure are subjected to similar specific requirements concerning CIP within their particular sectors of activity so that competition within the internal market is not distorted. EPCIP should minimise as much as possible any negative impact that increased security investments might have on the competitiveness of a particular industry. In calculating the proportionality of the cost, one must not lose sight of the need to maintain stability of markets that is crucial for long-term investment, the influence security has on the evolution of stock markets and on the macro-economic dimension.
- Ensure that Member States identify and address critical infrastructure under their jurisdiction, and especially critical infrastructure which if disrupted or destroyed could have an effect on other Member States or the entire EU.
    - Encourage the Member States to create national CIP programmes
    - Participate in the identification and designation of particular infrastructure as national and/or European critical infrastructure
- Ensure EU level coordination and cooperation concerning the protection of critical infrastructure
    - Create a CIP contact group representing all Member States
    - Agree on common definitions
    - Exchange best practices
    - Designate critical infrastructure which could be of importance to the entire EU, to two or more Member States or to a single Member State if the critical infrastructure is situated in another Member State.
    - Identify interdependencies

- Ensure the security of all sensitive CIP data

Consistency with other EU policies

A proposal to create a European Programme for Critical Infrastructure Protection is consistent with other EU policies. In particular, several other sectoral policies, including transport and energy, are already taking forward work at a sectoral level concerning CIP. These sectoral policies rely to a certain extent on the creation of a horizontal programme which would make sure that consistent approaches to the issue are developed.

Section 4: Policy options

- Option 1: refrain from addressing CIP issues at a European level. Under this option no horizontal actions would be undertaken at European level and the Member States would be left to address the issue individually. This approach has been disqualified by all Member States who generally see a need to address the issue from a European perspective.
- Option 2: the creation of a non-binding framework. Under this option a non-binding horizontal framework would be created at European level, but the Member States would be free to decide whether they want to make use of it.
- Option 3: the creation of a light legislative framework. Under this option, a number of binding measures would be implemented at European level. The Member States would be subjected to certain general obligations, but strong emphasis would still be put on the exchange of best practices, dialogue and the building of trust at EU level. The use of a Directive as the preferred legal instrument in this regard, would allow the Commission to make key issues obligatory for the Member States, but would give them the necessary freedom to adapt these obligations to their legal systems and CIP traditions.

  The Directive would respect national competences of the Member State and existing Community competences. Moreover, the sectoral competences of Commission services would be respected and relevant services would be expected to take forward sector specific work on critical infrastructure protection. The Directive would address such issues as:

  1. Set the objective of EPCIP and provide common general definitions
  2. Set the scope of EPCIP (all-hazards approach with a terrorism priority)
  3. Set out a list of critical infrastructure sectors relevant for EPCIP and a procedure for its amendment
  4. Set out how EPCIP would be implemented through the use of three work streams (the first on strategic issues, the second on European Critical Infrastructure, the third on National Critical Infrastructure)
  5. Oblige the Member States to designate CIP Contact Points who would coordinate CIP issues within each Member State and would participate in the EPCIP implementation work streams
  6. Oblige the Member States to elaborate National Critical Infrastructure Protection Programmes and to identify critical infrastructure under their jurisdiction
  7. Set out the procedure for the designation of European Critical Infrastructure
  8. Set out the procedure for developing specific protection measures for European Critical Infrastructure if such are required
  9. Set out the responsibilities of the owners/operators of critical infrastructure, in particular the designation of a Security Liaison Officer and the elaboration of an Operator Security Plan
  10. Set out the main rights of the owners/operators of critical infrastructure and the support available to them
  11. Provide a framework for the exchange of sensitive information and trust building measures.
  12. Set out an evaluation and monitoring mechanism.

- Option 4: full harmonization at EU level. Under this option, full harmonization measures would be proposed at EU level concerning the organization of CIP issues in the Member States as well as regarding the protection requirements relevant to the owners/operators of critical infrastructure. This approach may be contrary to the subsidiarity and proportionality principles and would be rejected by all Member States.

Apart from the four distinct options listed above, a combination of options 2 and 3 could be used to setup EPCIP. Under such an approach, the overall EPCIP framework and supporting measures would be addressed by way of a non-binding instrument. A number of core issues, in particular concerning ECI, would however be subject to a binding approach. The assessment of this approach will be performed in section 7.

Section 5: Analysis of impacts of general policy

The impact of particular policy options on specific issues is measured below as a function of the magnitude of the impact and its likelihood. The magnitude of each impact should be viewed as the level of influence a particular policy option would have on specific issues falling within the economic, environmental and social context. The likelihood of an impact is the probability that this impact will occur.

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
No impact	0

Option 1: refrain from addressing CIP issues at a European level.

Economic impacts

- *Costs for businesses.* If nothing was to be done at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to varying approaches and protection requirements depending on the Member State in which they operate. As a consequence businesses would have to invest in varying protection measures in order to comply with obligations imposed by various Member States. Although it is likely that most (if not all) Member States will implement their own approaches to CIP resulting in increased costs for all owners/operators of CI (who will have to upgrade their protection measures in order to comply with national obligations), the greatest costs would be borne by businesses operating in more than one Member State. There would be a high risk that costs would increase disproportionately for such businesses, as they would have to comply with different CIP obligations in each of the Member States in which they operate. This trend would likely increase if nothing was done at EU level. Moreover, the existence of several different CIP regulatory environments in the EU would increase a feeling of insecurity among investors, consumers and other stakeholders which could lead to less investor and consumer confidence in the long term (i.e. the industry benefits from a secure environment, consumer and customer trust, etc.).
    - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
        - Likelihood: √√√
    - Magnitude of the negative impact on the costs for businesses operating in more than one MS: - - -
        - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. These costs are associated with the need to create administrative structures dealing with CIP, hiring specialists etc. The likelihood of Option 1 having an impact on public authorities would be high, as most Member States see the need to address CIP issues. The magnitude of the impact would be medium.
    - Magnitude of the negative impact on the costs for authorities: - -
        - Likelihood: √√√
- *Negative impact on competition.* Competition may be affected as each Member State will impose different security obligations on businesses. Depending on the Member State, some companies will therefore have to invest more in security while others less. This would mean that businesses operating in certain Member States would be subjected to different obligations (and associated costs) despite the fact that they operate in similar or identical sectors. Moreover, the introduction of varying security standards in the EU Member States may constitute a significant barrier to entry into particular markets, especially for SMEs. The likelihood of this impact occurring would be high. The magnitude of the impact would also be high.
    - Magnitude of the negative impact on competition: - - -
        - Likelihood: √√√
- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Option 1 would most likely not have a big effect on the stimulation of research activities. It would also be unlikely to promote greater resource efficiency as the existence of numerous approaches to CIP in the Member States would make the setting of priorities difficult.
    - Magnitude of the impact on the stimulation of research activities: +
        - Likelihood: √
    - Magnitude of the impact on promoting greater resource efficiency in relation to research: +
        - Likelihood: √

Environmental impacts

Positive impact in terms of reducing environmental risks. The implementation of some form of CIP policy in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). Nevertheless, the lack of coordination and of a common approach to the protection of key infrastructure in Europe would mean that the likelihood of Option 1 having an impact on the prevention of certain risks and consequences would be low. The magnitude of the impact (if it

occurred) would be medium as certain vulnerabilities, especially concerning cross-border infrastructure, could not be protected against sufficiently through Option 1.

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: ++
  - Likelihood: √

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help increase the security of CI in Europe and thereby of the entire EU. As there would be no common approach/obligation to implementing CIP policies, some Member States would most likely remain more advanced than others. Consequently, the general level of protection of critical infrastructure would most likely be insufficient (system is only as strong as its weakest link). The lack of a common approach to the protection of critical infrastructure having a European importance would also be counter productive in terms of decreasing vulnerability. The likelihood of Option 1 having an impact on EU security is high. The magnitude of the impact however on increasing security would be low.
  - Magnitude of the impact on increasing EU security: +
    - Likelihood: √√√
- *Stakeholder involvement*. Various stakeholders including businesses, associations, standards authorities and public authorities need to be involved at all level (national and EU) in the development of CIP policies. Under Option 1, the involvement of stakeholders in the development and implementation of CIP policies across the Member States would be varied. In some Member States this involvement would be high, in others lower. Only a limited dialogue would take place at EU level. The likelihood of Option 1 having an impact on stakeholder participation is low. The magnitude of the impact of option 1 in this regard would also be low.
  - Magnitude of the impact on stakeholder involvement: +
    - Likelihood: √
- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 1 would mean that Member States would be completely free to address CIP issues as they see fit. Those Member States which have not yet started to deal with CIP issues, would of course need to adapt their administrative setup to a greater degree than those Member States which are already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to make certain modifications to their administrative setup in order to cope with the new responsibilities. The likelihood of Option 1 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup: - -
    - Likelihood: √√

- *Positive impact on employment and labour markets.* Employment and labour markets would generally remain unaffected by the adoption of Option 1.
    - Magnitude of the impact on employment and labour markets: 0
        - Likelihood: 0
- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 1 would not facilitate any significant trust building at EU level. At national level, trust building would depend entirely on the approach adopted by each MS.
    - Magnitude of the impact on building trust among stakeholders: +
        - Likelihood: √
- *Improved protection of national critical infrastructure.* The adoption of Option 1 would imply that each Member State would concentrate on improving the protection of its own critical infrastructure, which would undoubtedly result in higher levels of security. Nevertheless, it must be kept in mind that most national critical infrastructure do not operate in a vacuum – they can still be influenced by infrastructure existing in other Member States or from outside the EU (by way of various interdependencies). Consequently, Option 1 would be likely to improve the protection of national critical infrastructure, but the magnitude of the improvement would only be low.
    - Magnitude of the impact on improving the protection of national CI: +
        - Likelihood: √√
- *Improved protection of European critical infrastructure.* The adoption of Option 1 would not foresee the possibility of identifying European critical infrastructure and would not facilitate improving the protection of CI's (in a coherent and coordinated fashion) having a European importance. Due to the lack of any coordinated approach to the identification and protection of European critical infrastructure, their vulnerability would increase.
    - Magnitude of the impact on improving the protection of European CI: +
        - Likelihood: √
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 1 would be unlikely to improve such exchanges, and in particular of making them available to all EU Member States. Some bilateral/multilateral cooperation schemes are most likely already taking place and would continue.
    - Magnitude of the impact on improving the exchange of best practices: +
        - Likelihood: √
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. By adopting Option 1, no coordinated effort concerning the identification of interdependencies would take place apart from existing and future research activities.
    - Magnitude of the impact on the identification of interdependencies: +

- Likelihood: √

Option 2: the creation of a non-binding framework

The creation of a non-binding framework would most likely have a better impact on improving the protection of critical infrastructure in Europe than Option 1. Option 2 would create a basic framework for cooperation at EU level, which could facilitate the exchange of best practices. Nevertheless, the Member States would still be free to decide as to the level of their participation in CIP activities, which could prevent certain states from taking the necessary measures in the CIP field (due for example to the costs involved). Infrastructure which could have an impact on more than one Member States as well as cross-border infrastructure would therefore not be protected to a satisfactory extent.

Economic impacts

- *Costs for businesses.* If a non-binding framework was created at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would still be subjected to varying approaches and protection requirements depending on the Member State in which they operate (as under Option 1). In the short to medium term, the magnitude of the impacts as well as the likelihood would be the same as under Option 1 for both businesses operating in a single Member State and in more than one Member State. In the long term, as Member States increasingly discuss and cooperate on CIP issues, which could lead to the voluntary adoption of similar standards, the magnitude of the negative impact for businesses operating in more than one Member State could fall to medium. As there remains a certain amount of uncertainty whether such cooperation/coordination will actually occur to a satisfactory degree, the likelihood that costs for businesses would fall in the long term as compares to the short-medium term would be medium.
    - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
        - Likelihood: √√√
    - Magnitude of the negative impact on the costs for businesses operating in more than one MS:
        - In the short to medium term: - - -
        - In the long term: - -
        - Likelihood:
            - In the short to medium term: √√√
            - In the long term: √√
- *Costs for authorities.* The creation of a non-binding framework should have a more positive effect than Option 1 on enticing the Member States to improve the protection of their critical infrastructure in a cooperative fashion. As the framework would be non-binding, the actual results may nevertheless be smaller than expected. In terms of costs for the authorities, the adoption of Option 2 would have a similar impact as Option 1 (medium). The likelihood of Option 2 having an impact would however be low as costs would not be directly associated with the implementation of the common framework, but would rather stem from national approaches to CIP already being implemented.

- Magnitude of the negative impact on the costs for authorities: - -
    - Likelihood: √

- *Negative impact on competition.* The consequences of adopting Option 2 would most likely be similar to Option 1. Nevertheless, Option 2 could lead to greater cooperation and coordination among the Member States. As a consequence, it may be possible to adopt similar protection measures at least in certain Member States or sectors. The likelihood therefore of having competition suffer within the internal market would drop to medium as compared to Option 1. The magnitude would remain high.
    - Magnitude of the impact on competition: - - -
        - Likelihood: √√

- *Innovation and research.* Option 2 would have a more positive impact on innovation and research than Option 1 as the Member States would cooperate more closely through the non-binding framework. Due to the existence of a common framework and the possibility of having similar protection measures, Option 2 would be likely (medium) to stimulate research activities. The magnitude of the impact would remain low nevertheless. Option 2 would be more likely to promote greater resource efficiency than Option 1, as the existence of a common CIP framework would help Member States agree on priorities. The magnitude of the impact would remain low however.
    - Magnitude of the impact on the stimulation of research activities: +
        - Likelihood: √√
    - Magnitude of the impact on promoting greater resource efficiency in relation to research: +
        - Likelihood: √√

Environmental impacts

Positive impact in terms of reducing environmental risks. The implementation of some form of CIP policy in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a light coordination system and of a basic common approach to the protection of key infrastructure in Europe under Option 2 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be medium. The magnitude of the impact (if it occurred) would be medium (similar to Option 1).

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: ++
    - Likelihood: √√

Social impacts

- *Increasing security in the EU.* Option 2 would have similar impact as Option 1 in terms of helping increase the security of critical infrastructure in Europe and thereby of the entire EU. This option envisages that would only be a non-binding framework concerning CIP with no obligations concerning the implementation CIP policies. Consequently, some Member States would most likely remain more advanced than others. The general level of protection of

critical infrastructure would therefore most likely be insufficient (the system is only as strong as its weakest point). The likelihood of Option 2 having an impact on the security of critical infrastructure is high. The magnitude of the impact however on increasing security would be low.

- Magnitude of the impact on increasing EU security: +
  - Likelihood: √√√

- *Stakeholder involvement*. Option 2 could potentially have a better effect on stakeholder involvement than Option 1, especially at European level. The involvement of stakeholders in the development and implementation of CIP policies across the Member States would remain varied. In some Member States this involvement would be high, in others lower. Option 2 could nevertheless provide a basic system of dialogue at EU level with relevant stakeholders. The likelihood of Option 2 having an impact on stakeholder participation is nevertheless low. The magnitude of the impact of option 1 in this regard would be medium.
  - Magnitude of the impact on stakeholder involvement: ++
    - Likelihood: √
- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 2 would mean that despite the existence of a non-binding framework, Member States would be free to address CIP issues as they see fit. Those Member States which have not yet started to deal with CIP issues would of course need to adapt their administrative setup to a bigger degree than those Member States which area already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to make certain modifications to their structures in order to cope with the new responsibilities. The likelihood of Option 2 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - -
    - Likelihood: √√
- *Positive impact on employment and labour markets.* Employment and labour markets would generally remain unaffected by the adoption of Option 2.
  - Magnitude of the impact on employment and labour markets: 0
    - Likelihood: 0
- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 2 would go a long way in terms of building trust, especially at EU level (stakeholders would gradually be involved in discussions concerning CIP issues). At national level, the non-binding framework could be used as a basis to start regular discussions with stakeholders, which over time, would help build trust among those involved. Nevertheless, at national level, trust building would depend entirely on the approach adopted by each MS.
  - Magnitude of the impact on building trust among stakeholders: +++

        - Likelihood: √√

- *Improved protection of national critical infrastructure.* The adoption of Option 2 would imply that each Member State would concentrate on improving the protection of its own critical infrastructure, which would undoubtedly result in higher levels of security. Thanks to the creation of a non-binding framework under Option 2, it would nevertheless be possible to take more into account interdependencies and the broader international scene when it comes to CIP. Consequently, Option 2 would be likely to improve the protection of national critical infrastructure, but the magnitude of the improvement would only be medium.
    - Magnitude of the impact on improving the protection of national CI: ++
        - Likelihood: √√
- *Improved protection of European critical infrastructure.* Option 2 would foresee the possibility of identifying European critical infrastructure and cooperating on their protection. Option 2 would therefore have a more positive effect on the protection of European critical infrastructure than Option 1. The nature of the non-binding framework would mean nevertheless, that full cooperation may not be possible between the Member States in this regard (Member State may not want their infrastructure designated as European CI due to the costs involved etc).
    - Magnitude of the impact on improving the protection of European CI: ++
        - Likelihood: √√
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 2 would facilitate such cooperation. The magnitude of the positive impact could reach a high level as stakeholders would increasingly cooperate and have an interest in exchanging experiences and best practices under the voluntary framework. The likelihood would nevertheless remain low (as under Option 1) as it remains uncertain whether such exchanges would actually take place.
    - Magnitude of the impact on improving the exchange of best practices: +++
        - Likelihood: √
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 2, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information.
    - Magnitude of the impact on the identification of interdependencies: ++
        - Likelihood: √√

<u>Option 3: the creation of a light legislative framework.</u>

The creation of a light legislative framework would most likely have a better impact on improving the protection of critical infrastructure in Europe than Option 2. A number of basic legal obligations of a horizontal nature would be put on the Member States and the owners/operators of critical infrastructure with a view to improving the protection of critical infrastructure. At the same time, the framework would be light enough to encourage dialogue and the building of trust between CIP stakeholders and could therefore have a positive effect on

future developments related to EPCIP. The strong side of this approach would be that all Member States would have to make an effort to improve the protection of critical infrastructure and would be able to do so by building on their existing systems. Even those Member States which are currently least prepared in the CIP field, would have to implement certain measures so as to increase the security of their critical infrastructure and by doing so increase the security of the entire EU.

Option 3 would be more likely to improve the situation of the private sector as more predictability and similarity concerning CIP measures among the Member States could be expected. Consequently, the owners/operators would be subjected to similar requirements in each of the Member States, which would be particularly beneficial for cross-border infrastructure.

In general terms, Option 3 would create the overall framework on how to address CIP issues from a European perspective and would put in place a limited number of mainly procedural obligations intended to facilitate the process of improving the protection of critical infrastructure. Under this option, specific protection measures would be developed at a later stage following a process elaborated in the framework, which would guarantee compatibility between national approaches.

Economic impacts

- *Costs for businesses.* If a light binding framework was created at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to similar approaches and to common minimum protection requirements in each of the Member State in which they operate. As a consequence businesses would have to invest in similar basic protection measures in order to comply with obligations imposed by the Member States. Businesses operating in more than one Member State would particularly benefit from this situation, as they would have to comply with similar CIP obligations in each of the Member States in which they operate. The magnitude of the impacts would be similar for both businesses operating in a single Member States and in more than one Member State. The likelihood of having an impact on costs for businesses operating in a single MS would remain high. The likelihood would be high that the costs for businesses operating in more than one MS would fall (as compared to Options 1 and 2) as these businesses would be able to take advantage of economies of scale. Despite the differences mentioned above, all infrastructure designated as national or European critical infrastructure would be subjected to at least two cost-incurring obligations: the designation of a Security Liaison Officer and the elaboration of an Operator Security Plan. It is not possible to quantify these costs as they will depend on the sector concerned and the infrastructure itself. It is safe to say however, that the costs stemming from these obligations should be relatively low as:
    - Infrastructures likely to be designated as national or European critical infrastructure most likely already have security officers. Consequently, the obligations imposed under the EPCIP framework would amount to giving an already existing security officer some additional tasks
    - The vast majority if not all of the infrastructure likely to be designated as national or European critical infrastructure already prepare business continuity plans. Such plans would be very similar in nature to the proposed Operator Security Plans.

  In other words, although a number of potential critical infrastructure already possess functions similar to SLOs and OSPs, the adoption of Option 3 would create an obligation to this effect on all infrastructure designated as national or European critical infrastructure. The

designation of SLOs and the creation of OSPs would not in itself be an objective of EPCIP under Option 3. It would be a means of achieving the overall objective of EPCIP, that is, to increase the security of critical infrastructure in Europe. It should also be underlined that although specifically consulted on these options during the EPCIP Green Paper consultation, none of the responses provided concrete figures or raised specific concerns as to the costs that these obligations could entail.

Other obligations which could cause additional costs (for e.g. concerning new protection measures etc.) would be developed as needed on a sector-by-sector basis and could be quantified then. It is worth mentioning nevertheless, that several sectors are already well prepared to cope with a number of different risks. In many cases therefore, the implementation of EPCIP will not imply big additional costs.

The costs for businesses mentioned above would be counter-weighed by a number of rights bestowed upon the owners/operators of national or European critical infrastructure. These could include access to best practices, access to EU CIP funding, participation in the development of specific measures under EPCIP.

Moreover, the possible costs involved would at least be counter weighed by increased security, which means more stability, predictability and an increase in consumer confidence for the business environment, thus resulting in an increase in business opportunities and investments. Finally, as a consequence, potential new entrants will benefit as they will be faced with a foreseeable legal environment across the 25 Member States.

- Magnitude of the negative impact on the costs for businesses operating in a single MS: -
  - Likelihood: √√√
- Magnitude of the negative impact on the costs for businesses operating in more than one MS: -
  - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. The likelihood of Option 3 having a direct impact in this regard is medium (all Member States would have to have the necessary administrative structures in order to implement the common framework; several Member States however already have relevant structures in place). The magnitude of the impact of Option 3 would be medium as costs would not be directly associated with the implementation of the common framework, but would rather stem from national approaches to CIP already being implemented. The designation of CIP Contact Points should also not be viewed as an additional cost, as a vast majority of Member States (23) have already designated such contact points. The costs for administrations resulting from the adoption of the light binding framework could stem from:
  - The obligation to designate CIP Contact Points (as mentioned above, most Member States have already done so)
  - The obligation for each Member State to identify critical infrastructure under their jurisdiction (several Member States have already done this or are in the process). It would be difficult to quantify these costs as they depend on the approach adopted by

each Member State (whether it is the relevant authorities who identify the CI or is there an obligation on owners/operators to inform the relevant authorities about potential criticality), its size and the definition of what constitutes a national critical infrastructure.

- The obligation for each Member State to elaborate a National CIP Programme. Once again, several Member States already prepare such programmes. The process would nevertheless fall within the regular administrative activities of public authorities in a Member State.

Even, if certain administrative costs would prove to be necessary for the public authorities, these costs could legitimately be expected to be far outweighed by the benefits gained from increased security. These benefits, although not quantifiable, would touch upon the business environment, public confidence etc.

- Magnitude of the negative impact on the costs for authorities: - -
  - Likelihood: √√

- *Negative impact on competition.* Competition within the internal market is less likely to suffer if similar minimum protection requirements concerning critical infrastructure are implemented in each Member State. If security requirements are similar in all Member States, businesses will have to make similar investments. As a consequence, it will be unlikely that businesses in certain Member States will have to invest less due to security reasons. Of course, certain Member States may nevertheless decide to implement security obligations which go further than the minimum measures imposed by the common framework. The likelihood that competition would suffer as result of a light binding framework being adopted would be low. The magnitude of the impact would also be low.
  - Magnitude of the impact on competition: -
    - Likelihood: √

- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Due to the existence of a common framework and the possibility to agree on research priorities, Option 3 would be likely (high) to stimulate research activities. The magnitude of the impact would be medium as stakeholders would be more likely to invest in CIP if there was a common approach to the issue and agreed minimum levels of protection among the Member States. Option 3 would be more likely (high) to promote greater resource efficiency than Options 1 and 2, as the existence of a common binding CIP framework would help Member States agree on priorities. The magnitude of the impact would be medium.
  - Magnitude of the impact on the stimulation of research activities: ++
    - Likelihood: √√√

- Magnitude of the impact on promoting greater resource efficiency in relation to research: ++
    - Likelihood: √√√

Environmental impacts

Positive impact in terms of reducing environmental risks. The implementation of a common binding CIP framework in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a coordination system and of a basic binding common approach to the protection of key infrastructure in Europe under Option 3 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be high. The magnitude of the impact (if it occurred) would be high as various risks could be avoided due to increased cooperation built on the common framework (e.g. breakdowns of interdependent infrastructure located in different Member States).

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: +++
    - Likelihood: √√√

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help decrease security risks concerning CI and increase the security of the EU. As there would be a binding CIP framework in the EU, the Member States would share a minimum level of security concerning their critical infrastructure which would be high enough to limit associated risks. Despite the existence of minimum protection measures, the Member States could still implement higher measures than those required by the common framework. Consequently, the general level of protection of critical infrastructure would most likely be sufficient, which would help safeguard the security of the EU and its citizens. The likelihood of Option 3 having an impact on the security of the EU is high. The magnitude of the impact on increasing security would also be high.
    - Magnitude of the impact on increasing EU security: +++
        - Likelihood: √√√
- *Stakeholder involvement*. The involvement of stakeholders in the development and implementation of CIP policies across the Member States would be similar as the common binding framework would envisage stakeholder participation in the development and implementation of CIP measures. At EU level, stakeholder involvement would be guaranteed through the binding framework. The existence of a binding framework would moreover mean that all parties would be interested in participating in relevant CIP discussions (the results of the discussions could form the basis for future obligations). The fact that the framework would be light and that a step-by-step approach would be taken would further encourage dialogue and participation. The light binding framework envisaged under Option 3 would foresee the active involvement of Member State authorities, Commission services, owners/operators or critical infrastructure and standardisation bodies in the development of EPCIP. The likelihood of Option 3 having an impact on stakeholder participation is high. The magnitude of the impact of option 1 in this regard would be high.

- Magnitude of the impact on stakeholder involvement: +++
  - Likelihood: √√√

- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 3 would mean that Member States would have to address CIP issues taking due regard to the common binding CIP framework. Those Member States which have not yet started to deal with CIP issues would of course need to adapt their administrative setup more than those Member States which are already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to implement certain modifications to their structures in order to cope with the new responsibilities. The likelihood of Option 3 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - -
    - Likelihood: √√

- *Positive impact on employment and labour markets.* Employment and labour markets could be affected by the adoption of Option 3. Increasing demand for security technologies and CIP research, as well as the implementation of certain CIP requirements may create new jobs. Moreover, the adoption of Option 3 could contribute to the creation of new market segments associated with security. On the other, hand most companies likely to be designated as critical infrastructure already fulfil similar obligations and have the necessary personnel to do it (business continuity plans are prepared; security officers exist). The magnitude of the positive impact on the labour market would therefore be low. The likelihood of its occurrence would also be relatively low.
  - Magnitude of the impact on employment and labour markets: +
    - Likelihood: √

- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 3 could have a positive effect on building trust among stakeholders at national and EU level (stakeholders would gradually be involved in discussions concerning CIP issues). Public-private dialogue and in consequence the involvement of various stakeholders in CIP discussions at EU level, would be foreseen by the framework. The fact that CIP measures would be developed gradually and based on a sector-by-sector approach would mean that trust could be built over time. It is worth mentioning as well that in several sectors, relevant expert groups already exist, where sufficient levels of trust have already been achieved to share relevant information. Such expert group would be used to build EPCIP.
  - Magnitude of the impact on building trust among stakeholders: +++
    - Likelihood: √√

- *Improved protection of national critical infrastructure.* The adoption of Option 3 would imply that each Member State would continue working on improving the protection of its own critical infrastructure, while taking into account interdependencies and the broader cross-

border context. As a result, each Member State could take into account in its CIP process vulnerabilities stemming from the fact that infrastructure are interconnected. Consequently, Option 3 would be likely to improve the protection of national critical infrastructure, and the magnitude of the improvement would be high.

- Magnitude of the impact on improving the protection of national CI: +++
  - Likelihood: √√

- *Improved protection of European critical infrastructure.* Option 3 would provide a framework for the identification and protection of European critical infrastructure. The framework would foresee the identification of European CI and relevant protection measures on a sector by sector basis. Due to the fact that work would on identifying and protecting European CI would be taken forward on a step-by-step basis with the involvement of all stakeholders and through dialogue, Option 3 provides an ideal mix of voluntary and obligatory measures in the interest of increasing the protection of European CI.
  - Magnitude of the impact on improving the protection of European CI: +++
    - Likelihood: √√
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 3 would facilitate such cooperation by way of cooperation between Member States and other stakeholders in forums created for CIP purposes. The Commission would play a key role in this area in terms of gathering best practices and making them available to those Member States which require such assistance.
  - Magnitude of the impact on improving the exchange of best practices: +++
    - Likelihood: √√√
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 3, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information (like Option 2). The magnitude of the impact would therefore be high. The likelihood would be medium.
  - Magnitude of the impact on the identification of interdependencies: +++
    - Likelihood: √√

Option 4: full harmonization at EU level

The creation of a fully harmonized CIP system in the Member States would have a very strong effect on increasing the physical security of critical infrastructure in Europe, but would most likely be counter-productive in terms of building trust and dialogue among stakeholders. Consequently, the long-term development of EPCIP could be put at risk. On the economic side, the owners/operators of critical infrastructure would be subjected to identical requirements in all Member States which would significantly decrease their operational costs. This option has already been disqualified by most Member States and other stakeholders.

Economic impacts

- *Costs for businesses.* If full harmonization was attempted at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to

identical approaches and protection requirements in each of the Member State in which they operate. As a consequence businesses would have to invest in identical basic protection measures in order to comply with obligations imposed by the Member States. Businesses operating in more than one Member State would particularly benefit from this situation, as they would have to comply with identical CIP obligations in each of the Member States in which they operate. The magnitude of the impacts would be similar for both businesses operating in a single Member States and in more than one Member State. The likelihood of having an impact on costs for businesses operating in a single MS would remain high. The likelihood that Option 4 would have an impact on businesses operating in more than one Member State (costs would fall as compared to Options 1 and 2) would be high (such businesses would be able to take full advantage of economies of scale).

  - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
    - Likelihood: √√√
  - Magnitude of the negative impact on the costs for businesses operating in more than one MS: -
    - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. The likelihood of Option 4 having a direct impact in this regard is high as all Member States would have to have the necessary administrative structures in order to implement the harmonized approach (those Member States already have CIP structures in place would have to reform them in order to abide by the harmonized approach). Option 4 would moreover entail additional administrative costs associated with strict compliance monitoring. The magnitude of the impact of Option 4 would be high as costs would stem directly from the implementation of the harmonized approach, which would supplant existing national initiatives.
  - Magnitude of the negative impact on the costs for authorities: - - -
    - Likelihood: √√√
- *Negative impact on competition.* Competition within the internal market is less likely to suffer if identical protection requirements concerning critical infrastructure are implemented in each Member State. If security requirements are identical in all Member States, businesses will have to make identical investments. As a consequence, the risk of varying levels of investment in security will be avoided. The likelihood that competition would suffer as a result of the harmonized approach to CIP being adopted would be low. The magnitude of the impact would also be low.
  - Magnitude of the negative impact on competition: -
    - Likelihood: √
- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as

the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Due to the existence of a common harmonized framework and the possibility to agree on research priorities, Option 4 would be likely (high) to stimulate research activities. The magnitude of the impact would be high as stakeholders would be very likely to invest in CIP research considering that a harmonized approach exists and there are agreed levels of protection among the Member States. Option 4 would be more likely (high) to promote greater resource efficiency than Options 1 and 2, as the existence of a harmonized CIP framework would help Member States agree on priorities. The magnitude of the impact would be high as research could concentrate on the single harmonized approach.

- Magnitude of the impact on the stimulation of research activities: - - -
  - Likelihood: √√√
- Magnitude of the impact on promoting greater resource efficiency in relation to research: - - -
  - Likelihood: √√√

Environmental impacts

Positive impact in terms of reducing environmental risks.The implementation of a harmonized CIP framework in each Member State would reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a harmonized approach to the protection of key infrastructure in Europe under Option 4 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be high. The magnitude of the impact (if it occurred) would be high.

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: +++
  - Likelihood: √√√

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help decrease security risks concerning CI. As there would be a harmonized CIP framework in the EU, the Member States would have identical or similar levels of security concerning their critical infrastructure which would be high enough to limit associated risks. Nevertheless, the existence of a fully harmonized binding framework could also increase vulnerability as it could impede the building of trust among stakeholders, which is needed in order to comfortably exchange information on vulnerabilities. It is also true that having binding common levels of protection throughout the EU would mean that there might well be unnecessary protection measures put in place – or that there may be insufficient measures, as the threat levels are unlikely to be identical. The protection of critical infrastructure could then suffer. The likelihood of Option 4 having an impact on EU security is high. The magnitude of the impact on increasing security would be medium.
  - Magnitude of the impact on increasing EU security: ++

        - Likelihood: √√√

- *Stakeholder involvement*. The involvement of stakeholders in the development and implementation of CIP policies would be similar across the Member States as the harmonized framework would envisage stakeholder participation in the development and implementation of CIP measures. Nevertheless, the nature of the harmonization effort and the obligations imposed could discourage stakeholders from participating in the public-private dialogue as the potential outcome of such discussions would not have a sufficient effect on policy (most issues would have already been decided by way of the harmonization effort). The likelihood of Option 4 having an impact on stakeholder participation is medium. The magnitude of the positive impact of option 4 in this regard would be low (option 4 would be counterproductive).
    - Magnitude of the impact on stakeholder involvement: +
        - Likelihood: √√

- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 4 would mean that Member States would have to address CIP issues under the harmonized framework. All Member States would need to implement a certain number of modifications to their administrative structures. The likelihood of Option 4 having an impact on public administration is high. The magnitude would be high.
    - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - - -
        - Likelihood: √√√

- *Positive impact on employment and labour markets.* Employment and labour markets could be affected by the adoption of Option 4 similarly as under Option 3. A growing demand for security technologies and CIP research, as well as the implementation of certain CIP requirements may create new jobs. On the other hand most companies likely to be designated as critical infrastructure already fulfil similar obligations and have the necessary personnel to do it (business continuity plans are prepared; security officers exist). The magnitude of the impact would therefore be similar to that of Option 3. The likelihood of having a positive impact on employment markets would however increase to medium (as compared to Option 3).
    - Magnitude of the impact on employment and labour markets: +
        - Likelihood: √√

- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. This process, although highly desirable, cannot be forced. The adoption of Option 4 could have the potential to discourage various stakeholders from participating and contributing to the development of CIP (strong regulatory measures do not build confidence among stakeholders). The likelihood of this impact occurring would be high. The magnitude would be low (Option 4 would not help build trust).
    - Magnitude of the impact on building trust among stakeholders: +

        - Likelihood: √√√

- *Improved protection of national critical infrastructure.* The adoption of Option 4 would require each Member State to take a series of specific measures in relation to their critical infrastructure. This would improve the protection of national critical infrastructure in general. Nevertheless, the adoption of a harmonized approach could destroy what has already been built in some Member States in terms of CIP. As a result, general protection could suffer. Consequently, the magnitude of the impact in terms of improving the protection of national critical infrastructure would be medium under Option 4. The likelihood of the identified impact would be high. .
    - Magnitude of the impact on improving the protection of national CI: ++
        - Likelihood: √√√
- *Improved protection of European critical infrastructure.* Option 4 would provide a framework for the identification and protection of European critical infrastructure and would impose specific measures on how to protect them. The framework would foresee the identification of European CI and relevant protection measures on a sector by sector basis. Option 4 would be very likely to introduce strong protection measures for European critical infrastructure.
    - Magnitude of the impact on improving the protection of European CI: +++
        - Likelihood: √√√
- *Improving the exchange of best practices.* The adoption of Option 4 could facilitate the exchange of best practices as a harmonized cooperation framework would exist. Full harmonization established through Option 4 could however raise the question whether there would be any need to exchange best practices, in a situation when a single harmonized approach would be used. As a consequence, the magnitude of the impact could be described as medium. The likelihood of its occurrence would be high.
    - Magnitude of the impact on improving the exchange of best practices: ++
        - Likelihood: √√√
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 4, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information (like Option 3). Nevertheless, the likelihood would increase to high (as compared to medium under Option 3) as a coordinated effort would be made in this regard under the harmonized approach.
    - Magnitude of the impact on the identification of interdependencies: +++
        - Likelihood: √√√

Section 6: Comparing the options as to the general approach

Table of symbols

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
No impact	0

Summary table 1 – costs

Costs	Option 1 – no policy change	Option 2 – non binding framework	Option 3 – light legislative framework	Option 4 – full harmonization
Economic impacts				
Costs for businesses operating in a single Member State	- √√√	- √√√	- √√√	- √√√
Costs for businesses operating in more than one Member State	- - - √√√	Short/medium term: - - - Long term: - - Short/medium term: √√√ Long term: √√	- √√√	- √√√
Costs for authorities	- - √√√	- - √	- - √√	- - - √√√
Competition issues	- - - √√√	- - - √√	- √	- √
Social impacts				
Adaptation of the administrative setup	- - √√	- - √√	- - √√	- - - √√√

Summary table 2 – benefits

Benefits	Option 1	Option 2	Option 3	Option 4
Economic impacts				
Stimulation of research activities	+ √	+ √√	++ √√√	+++ √√√

Promotion of greater resource efficiency	+ √	+ √√	++ √√√	+++ √√√
Environmental impacts				
Reducing the likelihood or scale of environmental risks (fire, explosions etc)	++ √	++ √√	+++ √√√	+++ √√√
Social impacts				
Increasing EU security	+ √√√	+ √√√	+++ √√√	++ √√√
Stakeholder involvement	+ √	++ √	+++ √√√	+ √√
Employment and labour markets	0 0	0 0	+ √	+ √√
Building trust among stakeholders	+ √	+++ √√	+++ √√	+ √√√
Improved protection of national critical infrastructure	+ √√	++ √√	+++ √√	++ √√√
Improved protection of European critical infrastructure	+ √	++ √√	+++ √√	+++ √√√
Exchange of best practices	+ √	+++ √	+++ √√√	++ √√√
Identification of interdependencies	+ √	++ √√	+++ √√	+++ √√√

Advantages and drawbacks of the policy options

Policy options	Advantages	Drawbacks
Option 1: no policy change	▪ No need for new regulation. Regulatory environment does not change ▪ Member States remain completely free to address CIP issues as they see fit	▪ High costs for businesses operating in more than one Member State ▪ Competition may suffer as MS introduce various security obligations (companies in certain MS will have to spend less on CIP, while others more) ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ Small impact on improving EU security as accepted minimum

		levels of protection not achieved ▪ National and European CI not protected to a satisfying degree
Option 2: non-binding framework	▪ Trust can be built more easily among the stakeholders concerned ▪ No need for new regulation. Regulatory environment does not change ▪ Member States remain completely free to address CIP issues as they see fit	▪ High costs for businesses operating in more than one Member State ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ Competition may suffer as MS introduce various security obligations (companies in certain MS will have to spend less on CIP, while others more) ▪ Small impact on improving EU security as accepted minimum levels of protection not achieved
Option 3: light legislative framework	▪ Lower costs for businesses operating in more than one Member State ▪ Competition protected thanks to the existence of a minimum level playing field ▪ EU security strengthened ▪ Trust can be built more easily among the stakeholders concerned ▪ Improved protection of National and European CI	▪ Costs of establishment of new administrative structures ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ New regulatory environment is introduced.
Option 4: full harmonization	▪ Better stimulation of research activities and resource efficiency ▪ Improved protection of EU critical infrastructure ▪ Strong framework for the identification of interdependencies	▪ High costs of establishment of new administrative structures ▪ High costs of administrative reforms ▪ Difficult to build trust among stakeholders ▪ Risk of costs for businesses associated with the implementation of CIP measures

Would EU action have an added value?

As mentioned above, the European Council has already requested to Commission to prepare a European Programme for Critical Infrastructure Protection. The Member States therefore already see added value from EU level action in this regard.

Nevertheless, the analysis of the four policy options mentioned above confirms that action at European level would have an added value and is indeed needed. Each of the three policy options

which could be established at EU level (Options 2 to 4) could bring distinct benefits, but also a number of drawbacks.

Strengths and weaknesses of each policy option and preferred option

- Option 1. The "no policy change" option does not present any clear strengths in terms of improving the protection of critical infrastructure in Europe. It does present however a number of disadvantages stemming from competition issues, greater costs for businesses, insufficient security.
- Option 2. The "non-binding framework" option possesses the clear advantage of creating a framework designed to build trust among all stakeholders. This advantage cannot however balance out the strong disadvantages stemming from this option including growing costs, competition issues and the heightened security risk. The issue of security is a key problem of this Option. A non-binding framework will not provide the needed basis to have all Member States implement sufficient protection measures for their critical infrastructure.
- Option 3. The "light legislative framework" option provides the best balance of advantages and disadvantages. This approach would safeguard competition, lower costs for businesses operating in more than one Member State and increase security in the European Union. These clear advantages would seem to outweigh the disadvantages associated with costs. Another possible disadvantage of this option stems from the fact that it creates another regulatory framework in the EU. However, in the interest of security, this approach seems to be justified.
- Option 4. The "full harmonization" option creates several clear advantages and disadvantages. On the positive side, EU critical infrastructure would be protected to a high degree. On the downside, high costs would be involved and it would be difficult to build trust among stakeholders. Finally, this option has already been disqualified by the Member States, which want EPCIP to build on and complement their existing achievements.

Based on the analysis above, policy option 3, the creation of a light legislative framework, would be the best policy option.

However, taking into account the fact that EPCIP constitutes a completely new policy and that there is therefore a need for a step-by-step approach in the CIP field, the best practicable option would consist of a combination of options 2 and 3. The overall framework of EPCIP would thereby be addressed by a non-binding instrument, while a few key requirements concerning ECI would be introduced through binding measures.

Based on this assessment of broad policy options, the following section presents an assessment of possible contents of this framework.

Section 7: Analysis of impacts of specific measures under the recommended policy consisting of binding and non-binding measures

Overview

As set out above, the need for a comprehensive and consistent step-by-step approach to establishing EPCIP would merit a combination of binding and non-binding measures.

The following key issues could usefully be included in EPCIP:

- participation in CIP expert groups at EU level;
- use of a CIP information sharing process;
- identification and analysis of interdependencies;
- elaboration of national CIP programmes including the identification of national critical infrastructure;
- nomination of CIP Contact Points;
- identification and designation of European Critical Infrastructure;
- conducting threat and risk assessments for ECI
- elaboration of Operator Security Plans;
- designation of Security Liaison Officers.

Before analysing the specific impacts of the above mentioned key measures and assessing whether they should be implemented through non-binding or binding measures, it is useful to distinguish clearly between measures addressed to: a) the Member States, and/or b) to the owners/operators of ECI:

a) Member States: participation in CIP expert groups at EU level; use of a CIP information sharing process; identification and analysis of interdependencies; elaboration of national CIP programmes including the identification of national critical infrastructure; nomination of CIP Contact Points; identification and designation of European Critical Infrastructure; conducting threat and risk assessments for ECI.

b) ECI owners/operators: participation in CIP expert groups at EU level; use of a CIP information sharing process; identification and analysis of interdependencies; elaboration of Operator Security Plans; designation of Security Liaison Officers.

In the following section, for each of the key elements, the impacts of binding and non-binding instruments will be assessed. Since EPCIP's general objective is to improve the protection of critical infrastructure in the EU, the positive impact on security of the key elements will be weighed against the potential costs. In addition, in order to underline the importance of economic considerations, the potential impact on the functioning of the common market will also be assessed below.

Some elements can due to their nature only be addressed by non-binding measures, for example the setting up of expert groups. In these cases the assessment will be limited to the non-binding approach. As it is not possible at this time to assess what will be the level of participation of

stakeholders in these measures, it is also difficult to foresee potential costs. Nevertheless a number of general comments can be made concerning the key non-binding measures.

Analysis of impacts of key measures forming part of the EPCIP framework

1. *Participation in CIP expert groups at EU level.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. The use of EU level expert groups in order to bring together relevant stakeholders would greatly facilitate a CIP information exchange. Such CIP expert groups would have a very positive impact in terms of security as they could:

    - Assist in identifying vulnerabilities, interdependencies and sectoral best practices;
    - Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;
    - Facilitate CIP information-sharing, training and building trust;
    - Develop and promote "business cases" to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;
    - Provide sector-specific expertise and advice on subjects such as research and development.

    Costs would be limited as CIP expert groups would only be setup where needed and on a *pro bona* basis, and would not replace other existing groups already established or which could be adapted to fulfil the needs of EPCIP. Moreover, CIP expert groups would be formed in order to achieve a clearly identified objective and would be dissolved following its attainment.

    The creation of EU level expert groups would not have an impact on the Common Market.

    As EU level expert groups would function on a voluntary basis, they should form part of the non-binding framework of EPCIP. Binding measures would be contrary to the nature of such voluntary groups.

2. *Use of a secure CIP information sharing process.* The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that have been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. Supporting a voluntary CIP information exchange cannot be done by way of binding measures as these would be counterproductive in terms of building trust and facilitating dialogue. Consequently, a non-binding approach would be preferred.

    Making sure that the CIP information exchange is secure will of course have a positive impact on increasing security. Costs can be expected to remain low as the measures remain non-binding and are relevant more for an introduction of a certain security oriented "state of mind". Consequently, the process should amount to the development of guidelines on information handling etc.

3. *Identification and analysis of interdependencies.* The identification and analysis of interdependencies, both geographic and sectoral in nature, will be an important element of improving critical infrastructure protection in the EU. No binding measures can be imposed in this regard as the identification of interdependencies is part of a broader process which

requires cooperation and coordination between several stakeholders. A binding approach could therefore be counterproductive.

This ongoing process will feed into the assessment of vulnerabilities, threats and risks concerning critical infrastructure in the EU and may therefore have a significant impact on security. An estimation of costs cannot be made at this time as the process of identifying interdependencies is of an ongoing nature. It is worth underlining nevertheless that EU funding could contribute to this process by way of calls for proposals.

4. *Elaboration of National CIP Programmes.* Raising CIP capability and improving the protection of critical infrastructure in the EU are objectives of EPCIP. While clearly the responsibility for protecting National Critical Infrastructure falls on the NCI owners/operators and on the Member States, there would also be a Community benefit in making sure that the issue of National Critical Infrastructure is being sufficiently addressed in each of the Member States. The Commission should support the Member States in their NCI related efforts where requested and where possible.

   The impact of NCI related measures on security and costs will of course be different depending on whether a binding or non-binding approach to NCI is introduced in EPCIP.

   - Impact of a binding approach concerning the elaboration of National CIP Programmes. Under this scenario, EPCIP would oblige each Member State to create a National CIP Programme based on a number of minimum general requirements and on the list of CI sectors relevant for EPCIP. This obligation would be put forward in EPCIP in order to ensure that each Member State develops a coherent national approach to CIP and that this national approach is compatible with EPCIP (and thereby with the approaches of the other Member States). The relevant binding provisions would nevertheless be general enough to allow each Member State to make use of national specificities.

     - Security. In terms of the impact on security, the elaboration of National CIP Programmes under a binding framework could be expected to have a strong effect on increasing the security of critical infrastructure in Europe because:

       - All Member States would be required to establish National CIP Programmes addressing similar issues. This would mean that those Member States which already have such programmes would have to assess whether they fulfil the common minimum requirements under EPCIP. Those Member States which do not have such programmes would have to develop them.
       - Since all National CIP Programmes would address similar issues, the programmes would be compatible and comparable with each other.
       - Similarity between the National CIP Programmes in terms of the approach used would guarantee that each Member State is sufficiently addressing national CIP issues.

     - Costs. The costs associated with National CIP Programmes should be separated into two distinct phases: the elaboration phase and the implementation phase. The costs of both phases would vary in each Member State.

       - The elaboration phase would be limited to the drafting of the National CIP Programmes. This phase would therefore only require funding concerning the

elaboration of a national approach to CIP. It should be expected that this work can be fulfilled by the regular administrative structures usually dealing with CIP in a particular Member State. Those Member States which already have relevant programmes would simply need to make sure that they take into account the minimum common requirements. Those Member States which would have to elaborate a completely new programme would have to incur higher costs, although these would generally be of an administrative nature. Although quantification of this process is not possible at this time, the costs should be expected to remain low during this phase.

- The implementation phase would require a higher degree of funding. The costs would vary among the Member States depending on the level of advancement on CIP issues (e.g. several Member States have already identified their National Critical Infrastructure and are already engaged in dialogue with CI owners/operators). Importantly nevertheless, some of the minimum requirements of the National CIP Programmes specified in the EPCIP proposal could be funded by the Commission (e.g. studies on interdependencies).

- There would be no direct impact on the functioning of the common market as a result of this obligation. Indirectly however, the fact that comparable programmes would be setup concerning NCI would lead to similarities in protection measures concerning NCIs. This in turn would help approximate national security requirements for NCIs (level playing field).

➢ Impact of a non-binding approach concerning the elaboration of National CIP Programmes. Under this scenario each Member State would be encouraged to create a National CIP Programme. A non-binding instrument would propose a number of issues which could be taken into account by the Member States when developing such programmes including the identification of NCI.

- Security. In terms of the impact on security, the elaboration of National CIP Programmes could be expected to have a positive impact on increasing the security of critical infrastructure in Europe as each Programme would set out a Member State's strategy toward CI protection and would confirm that the issue is being addressed to a certain extent. At the very minimum, such Programmes would serve as a good awareness raising tool. The positive impact on security could however be expected to be lower than under a binding approach as the Member States would most likely develop a number of approaches to the protection of National Critical Infrastructure which may be incompatible between each other. This would hinder certain forms of cooperation (e.g. exchange and comparability of certain types of information). Moreover, certain Member States could refrain from developing such programmes.

- Costs. The costs associated with National CIP Programmes cannot be assessed as the approaches of the Member States will vary. Nevertheless, the elaboration costs can be expected to remain low. Implementation costs will depend on the ultimate contents.

- There would be no impact on the functioning of the common market.

Although having clear security benefits, the introduction of a binding approach to National CIP Programmes may not be possible at first. Subsidiarity and the need for a step-by-step approach to EPCIP may justify the concentration of binding measures on ECI related issues.

In conclusion, the use at first of a non-binding approach to National CIP Programmes may be justified. This approach would however have to be re-assessed once work progresses on the issue of ECI.

5. *Identification of national critical infrastructure by each Member State.* The identification of National Critical Infrastructure is a prerequisite for making sure that they are being adequately protected. As mentioned above in the analysis of the need to create National CIP Programmes, either a binding or non-binding approach to NCI could be used in this regard.

   - Impact of a binding approach concerning the identification of NCI. Under this scenario, EPCIP would oblige the Member States to ensure the ongoing identification of National Critical Infrastructure. Such an obligation would be introduced in order to make sure that all Member States are aware of the critical infrastructure assets located within their territory and understand the potential consequences of the loss or disruption of such an infrastructure. In general terms, the Commission would not require specific information concerning these critical assets (with due regard to existing Community competences).

     - Security. The identification of national critical infrastructure by each Member State would have a very strong effect on improving the security of critical infrastructure in Europe. This would be the result of the fact that each Member State would have to go through a process of assessing which concrete infrastructure are critical for it and why. This would of course result in increasing the level of understanding of CIP issues within the Member States.

     - Costs. The costs of identification would vary among the Member States. Those Member States which have already identified their National Critical Infrastructure would not have to repeat the process. Those Member State which have not completed the necessary identification, would incur costs associated with the collection and analysis of the relevant data. The associated costs for infrastructure owners/operators would be very low as it can be reasonably expected that they already know what assets are critical for them. The costs would remain low.

     - This provision would not have an impact on the functioning of the common market.

   - Impact of a non-binding approach concerning the identification of NCI. Under this scenario, EPCIP would encourage the Member States to identify their National Critical Infrastructure, but the Member States would be under no obligation to do so.

     - Security. The non-binding approach would clearly have a lower security impact than a binding approach as there would be a risk that not all Member States would address the NCI issue sufficiently. Nevertheless, the need for a step-by-step approach to EPCIP and the need to concentrate on ECI may merit the use of a non-binding approach. The issue of encouraging the Member States to identify their NCI could then be integrated within the non-binding provisions concerning National CIP Programmes. Costs would vary depending on the types of actions undertaken by each particular Member State.

     - Costs. The costs of identification would vary among the Member States as under the binding measures.

     - This provision would not have an impact on the functioning of the common market.

In conclusion, the use of a binding approach concerning the identification of NCI would give stronger security benefits than a non-binding approach. Nevertheless, due to subsidiarity and the need to concentrate at first on ECI issues, the use of a non-binding approach to the identification of NCI may be justified. As the EU's experience in the CIP field grows, this approach may however have to be re-assessed.

6. *Nomination by each Member State of a CIP contact point.* There is a need for each Member State to designate a CIP contact point, who would have a general overview of CIP activities in the Member State and would coordinate CIP within the Member State and with other Member States, the Council and the Commission.

   - Impact of a binding approach concerning the nomination CIP contact points:

     - Security. From the security perspective, this provision is important as it envisages the designation of a horizontal CIP coordinator in each Member States, which would have a general overview of CIP related activities in that Member State and would function as the single point of contact on CIP issues. A horizontal overview of CIP activities is needed in order to encourage compatible and adequate approaches to CIP in all CIP sectors. In addition, the CIP Contact Points would represent the Member States in the Committee setup under a binding EPCIP instrument, which would take decisions on implementation measures under the binding instrument. The CIP Contact Points would also represent the Member States in the informal CIP Contact Group being setup under the horizontal EPCIP framework and would therefore contribute to the development of EPCIP. The nomination of a single contact point would be important in terms of building trust and facilitating discussions on CIP issues at the EU level.

     - Costs. The cost of nominating a single CIP contact point will vary in each Member State as a consequence of different administrative structures and salary levels. In general terms, two situations should be differentiated:

       - A civil servant already employed by the public administration and already dealing with CIP issues is nominated as the CIP Contact Point. The costs here would be negligible as the necessary structures would already be in place. The coordinating role of the Contact Point would require the establishment of contacts with all the relevant CIP authorities in a particular Member States. This would be the case for most of the Member States.

       - A new position is created within the public administration. Costs would vary between the Member States, but would generally result from the need to incur administrative costs.

       Costs can reasonably be expected to remain low as 23 Member States have already nominated their CIP contact points and have notified the names to the Commission.

     - This provision would not have an impact on the functioning of the common market.

   - Impact of a non-binding approach concerning the nomination CIP contact points on:

     Security. From the security perspective, the nomination of CIP Contact Points is crucial for the success of EPCIP. Without participation of all Member States in the process, the objective of improving the protection of CI in Europe will not be achieved. The main problem with a non-binding approach would be that the Member

States would be free to decide on whether to actually nominate such a Contact Point. The lack of even a single Member State in the EPCIP process would risk derailing the project. From this perspective the benefit for security of a non-binding approach would be low.

- Costs. The cost of nominating a single CIP contact point will vary in each Member State. The costs would be similar as under the binding approach given that a Member State would nominate a Contact Point.
- This provision would not have an impact on the functioning of the common market.

Consequently, only a binding approach would guarantee that each Member State performs the necessary tasks. Non-binding measures could be mildly successful, but could in no way guarantee that each Member State would nominate a CIP Contact Point. A binding approach to CIP Contact Point designation would therefore be preferred.

7. *Identification and designation of European critical infrastructure.* The identification and designation of ECI is at the heart of EPCIP, as improving the protection of critical infrastructure can only occur once the relevant infrastructure have been identified. This process needs to be completed in a coordinated fashion and can only be successful when undertaken at EU level. The identification and designation of European Critical Infrastructure could best be done based on a four step process:

    i. The development of criteria to identify ECI on a sectoral basis;

    ii. The adoption of the criteria

    iii. The identification by the Member States of those critical infrastructure which could satisfy the common criteria;

    iv. The formal designation of specific infrastructure as ECI.

This process would lead to the creation of a list of European critical infrastructure which if disrupted or destroyed would have serious consequences for the entire Community, two or more Member States, or a single Member State if the critical infrastructure is located in another Member State.

- Impact of a binding approach concerning the identification and designation of ECI:
  - Security. The security benefit of the identification and designation of ECI can be expected to be very big as this identification is a prerequisite for improving the protection of such infrastructure (if needed). This has to be done using a commonly agreed approach with the full participation of all Member States.
  - Costs. The costs involved would be small as they would generally be of an administrative nature associated with the holding of meetings and facilitating discussions especially in the criteria development phase.
  - This provision would not have an impact on the functioning of the common market.
- Impact of a non-binding approach concerning the identification and designation of ECI on:
  - Security. The potential security benefit would only be achieved if the process of identification actually took place. As it is unlikely that such a process could be

completed to a satisfactory degree under a non-binding approach the security benefit would be low.

- Costs. The potential costs would be the same as those under a binding approach.
- This provision would not have an impact on the functioning of the common market.

In conclusion, only a binding approach to the identification and designation of ECI can provide a high probability of success in terms of achieving EPCIP's objectives. Moreover, a binding approach in this regard would have two further positive consequences:

- transparency – if the identification and designation is subject to a legal procedure it is subject to scrutiny by Member States – and potentially by others, this way transparency is maximised.
- comparability – ensuring that there are common procedures and methods will mean that the ECI identified will be comparable, and will not be subject to potentially very different interpretations by Member States.

If a non-binding approach to this process would be used, the EU would be faced with a situation in which only certain European critical infrastructure having an EU importance would be identified. It is in the interest of the entire EU to eliminate such weak links.

8. *Conducting vulnerability, threat and risk assessments for ECI.* Each Member State should conduct a risk and threat assessment in relation to relevant ECI. Such assessments would be done in order to improve the protection of ECI as:

   - Relevant information concerning identified threats and risks could be communicated to the ECI via the Security Liaison Officer, thereby strengthening an ECI's CIP capacity.
   - The information would help the MS prepare the generic sectoral summaries of identified vulnerabilities, threats and risks which would be submitted to the Commission.

   ➢ Impact of a binding approach to conducting vulnerability, threat and risk assessments for ECI:

   - Security. The security benefit would be large as the Member State, the ECI owner/operator and the Commission could benefit from the vulnerability, threat and risk assessments and act upon it. The binding framework would foresee the use of this information in order to achieve greater CI security. All Member States would fully participate in the process so weak links would be eliminated to the highest possible extent.
   - Costs. The costs of conducting such assessments would vary among the Member States and among the various CIP sectors. Nevertheless, it can be expected that such assessments would be made as part of regular work conducted by law enforcement agencies of the Member States. The additional costs would therefore be low.
   - This provision would not have an impact on the functioning of the common market.

   ➢ Impact of a non-binding approach to conducting vulnerability, threat and risk assessments for ECI:

- Security. The security benefit would not be as significant as under the binding approach as there would be no binding provisions concerning the sharing and use of this information. It would therefore not be possible to conduct an EU level analysis of security gaps and it would not be possible to propose measures to address these gaps.
- Costs. The costs of conducting such assessments would vary among the Member States and among the various CIP sectors. Costs would remain low as under the binding approach.
- This provision would not have an impact on the functioning of the common market.

Due to this action's role in the entire process of strengthening the protection of ECI, the use of a binding instrument in this regard would be justified. Without making sure that all Member States conduct relevant assessments, the ECI owners/operators will not have sufficient information concerning potential threats and an EU level assessment of protection gaps could not be conducted. The essence of the European Programme for Critical Infrastructure Protection would be lost without the implementation of this measure.

9. *Obligations of European Critical Infrastructure.* In order to achieve the objective of improving the protection of ECI, two measures to be undertaken by the ECI owners/operators should be considered: the designation of a Security Liaison Officer and the elaboration of an operator security plan.

➢ Impact of binding obligations for ECI on:

- Security. Security would clearly benefit from these provisions as:
  - European critical infrastructure would have to complete the process of preparing Operator Security Plans which make sure that risk, threat and vulnerability assessments are sufficiently taken into account and that the owner/operator is aware of its critical assets and knows how best to protect them. The information from the OSPs would help the Member States elaborate generic reports concerning vulnerabilities, threats and risks to ECI, which would be submitted to the Commission with a view to identifying gaps in protection measures.
  - The designation of Security Liaison Officers would facilitate the CIP process as each owner/operator of European critical infrastructure would have a clearly identifiable official responsible for CIP issues. This official would not only be the single point of contact with the authorities concerning CIP, but would also contribute to the development of CIP policies by way of participating in expert/stakeholder meetings (building trust).
- Costs. The costs would vary among the Member States. Although exact quantification is not possible, the following assumptions can be made concerning the two above mentioned obligations:
  - The owners/operators of European critical infrastructure would incur costs associated with the preparation of Operator Security Plans. The exact costs will vary considerably depending on the sector concerned, the type of activities being undertaken, the level of preparedness already achieved. Costs can be expected to be low or non-existent for those owners/operators who:

- Have already prepared business continuity plans.
- Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to prepare Operator Security Plans already exists).
- Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[2] obliges port authorities to develop port security assessments and plans which would most likely already satisfy the obligations imposed through a sector specific Operator Security Plan).

Costs can reasonably be expected to be higher for owners/operators who have not addressed security or business continuity issues at all. It could however be expected, that even without the adoption of EPCIP, certain costs concerning business continuity plans would be incurred at a certain point in the future. The problem would remain however that this would be done in an uncoordinated and incomparable fashion.

Recognising the need for a cost-effective system EPCIP should be based on a sectoral approach and should build on existing sectoral measures. With this in mind, the specific contents of the Operator Security Plans would be elaborated on an individual basis taking into account (where relevant) existing CIP sector specificities (e.g. port security assessments and plans under the Port Security Directive). A procedure would be established foreseeing the exemption of certain sectors from the obligation to elaborate OSPs.

- The owners/operators of European critical infrastructure would incur costs associated with the designation of Security Liaison Officers. As with the Operator Security Plans however, these costs will vary depending on a number of factors. Costs can be expected to be low or not to exist at all for those owners/operators who:
  - Already possess a security officer. For most owners/operators likely to be designated as ECI, this is most likely the case. In this situation, the designation of an SLO will simply amount to giving particular security officials additional competences.
  - Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to designate SLO already exists).
  - Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[3] already obliges the Member States to appoint port security officers for each port. Although

[2] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

[3] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

this is not identical to the designation of a SLO, which has to be done by the owners/operator, it can serve as a basis for such a designation).

Costs will of course be higher for those owners/operators which do not possess any security officers. Such a situation would however be relatively unlikely for owners/operators designated as European critical infrastructure.

- These obligations could have an impact on the functioning of the common market. Introducing similar obligations for all ECI would mean the existence of a level playing field for all ECI owners/operators in the EU. In other words, the use of binding measures would make sure that all ECI owners/operators are subject to the same rules as opposed to having varying obligations in particular Member States.

- Impact of non-binding obligations for ECI on:
  - Security. The security benefit would be low mainly as a consequence of the fact that only certain ECI owners/operators would comply with the obligations. This would hinder the process of improving the security of ECI as:
    - Without having each ECI develop OSPs, it will not be possible to conduct an analysis of gaps and it will not be possible to propose measures on how to address them. Moreover, without an OSP, it will be difficult to assess whether the ECI owner/operator is addressing security issues to a satisfactory degree, which raises the issue of having weak links in the security of the EU.
    - In relation to the designation of Security Liaison Officers, the fact that certain ECI owners/operators would not have SLOs would hinder the development of security measures as it would be difficult to ensure the needed communication concerning security issues. The lack of a specific person responsible for CI security would also hinder the process of building trust among stakeholders, which is needed in order to comfortable exchange information.
  - Costs. The costs would depend on whether the measures were actually implemented. If so, they could be assessed as under the binding approach. If no, then under a non-binding framework ECI owners/operators would still be subjected to varying basic obligations depending on the Member State in which they operate. This would lead to ECI owners/operators having to invest in different measures depending on the Member State in which they operate. The negative impact on costs could therefore even be larger than under the binding option.
  - The use of non-binding measures could have an impact on the functioning of the common market. As certain ECI owners/operators would implement the measures, others would refrain and would thereby gain a competitive advantage over others. The use of non-binding measures could also encourage the Member States to develop various incompatible obligations. Under such a scenario, ECIs could end up being subjected to a number of different security requirements in each of the Member States.

The use of a binding instrument concerning these two obligations is justified as it would not be possible to achieve a coherent approach to the protection of ECI across the EU in any other way. If non-binding measures were used, only a certain number of ECI would comply. The possible costs involved would at least be counter weighed by increased security, which means

more stability, predictability and an increase in consumer confidence for the business environment, thus resulting in an increase in business opportunities and investments.

Summary table

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Positive impact	+
Negative impact	-
No impact	+/-
Not applicable	n.a.

Key provision	**Binding approach**			**Non-binding approach**			**Other considerations**
	Impact on:			Impact on:			
	Security	Costs	Common Market	Security	Costs	Common Market	
Participation in CIP expert groups at EU level	n.a.	n.a.	n.a.	+++	+/-	n.a.	
Use of a CIP information sharing process	n.a.	n.a.	n.a.	+++	+/-	n.a.	
Identification and analysis of interdependencies	n.a.	n.a.	n.a.	+++	n.a.	n.a.	
Elaboration of National CIP Programmes	+++	-	+	+	n.a.	n.a.	Need to concentrate first on ECI
Identification of National Critical Infrastructure	+++	+/-	n.a.	+	+/-	n.a.	Need to concentrate first on ECI
Nomination of CIP Contact Points	+++	+/-	n.a.	+	+/-	n.a.	
Identification and designation of European critical infrastructure	+++	+/-	n.a.	+	+/-	n.a.	
Conducting threat and risk assessments for ECI	+++	+/-	n.a.	+	+/-	n.a.	
Designation of a Security Liaison Officer, elaboration of an operator security plan	+++	-	+	+	--	-	

Conclusions

The analysis of the specific impacts of the nine key measures suggests that a combination of binding and non-binding measures would be best suited to achieving the objectives of EPCIP while providing the best cost/benefit ratio.

In terms of the nine key measures analysed above, five would be better placed in a non-binding framework, while four should be made obligatory:

(I) Non-binding measures:

a) participation in CIP expert groups at EU level;

b) use of a CIP information sharing process;

c) identification and analysis of interdependencies;

d) elaboration of national CIP programmes

e) identification of national critical infrastructure;

(II) Binding measures:

a) nomination of CIP Contact Points;

b) identification and designation of European Critical Infrastructure;

c) conducting threat and risk assessments for ECI;

d) elaboration of Operator Security Plans; designation of Security Liaison Officers.

As a consequence, the recommended policy for the creation of EPCIP would consist of:

1. A general non-binding EPCIP framework set out in a Commission Communication
2. A binding instrument dealing specifically with ECI (ECI Directive).

As mentioned above, the horizontal non-binding EPCIP framework could be established by way of a Commission Communication. The Communication would clearly specify that EPCIP consists of:

1. A Directive concerning ECI
2. Non-binding measures designed to facilitate the implementation of EPCIP, including an EPCIP Action Plan, the use of CIP expert groups at EU level, CIP information sharing process and the identification and analysis of interdependencies.
3. A possible Critical Infrastructure Warning Information Network (CIWIN) (this will be the subject of a separate proposal)
4. Non-binding measures which may optionally be used by Member States for National Critical Infrastructure (NCI) under their responsibility
5. Accompanying financial measures set out in the EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" (financial perspectives for 2007-2013). This programme will provide funding opportunities for CIP related measures having a potential for EU transferability

A binding instrument concerning ECI would constitute a key element of the EPCIP package as set out in the EPCIP Communication. The instrument, which would take the form of a Directive, would only be limited to the identification and designation of European Critical Infrastructure, and to establishing a common approach to the assessment of the needs to improve the protection of such infrastructure.

In particular such a Directive would address the following issues:

1. The establishment of a procedure for the identification and designation of European critical infrastructure
2. The elaboration of an operator security plan and the designation of a Security Liaison Officer by each owner/operator formally designated as an ECI in order to conduct vulnerability, threat and risk assessments
3. The establishment of a reporting mechanism under which each Member State would provide the Commission with a generic overview of vulnerabilities, threats and risks encountered in each CIP sector.
4. The nomination by each Member State of CIP contact points.

In comparison with the light legislative framework foreseen under Option 3, this approach would introduce the following modifications:

1. The Directive would only be limited to establishing a procedure for the identification and designation of ECI and the assessment of their vulnerabilities
2. National Critical Infrastructure would be completely left out of the Directive. A general approach to NCI would be provided in the Communication on EPCIP, but the Member States would be free to decide whether such an approach would suite them.
3. The procedure for the development of specific protection measures would be completely left out of the framework. The development of such measures could be the objective of future policy and/or legislative exercises, if appropriate. The information gathered under the EPCIP framework could contribute to this process nevertheless (e.g. for the preparation of an impact assessment).

The number of CIP sectors included in the Directive would be reduced as certain NCI-relevant sectors would no longer be included.

Table 1: Binding and non-binding EPCIP measures and division of responsibilities among stakeholders

Key provision	**Stakeholder responsible**		
	Member State	European CI	EC
Non-binding measures			
Participation in CIP expert groups at EU level	√	√	√
Use of a CIP information sharing process	√	√	√
Identification and analysis of interdependencies	√	√	√
Elaboration of National CIP Programmes	√		
Identification of National Critical Infrastructure	√		
Binding measures			
Nomination of CIP Contact Points	√		
Identification and designation of	√		√

European critical infrastructure			
Conducting threat and risk assessments for ECI	√		
Designation of a Security Liaison Officer, elaboration of an operator security plan		√	

Proposed timeframe for implementation

1. The sectoral criteria for the identification of ECI would be adopted at the latest one year after the entry into force of the ECI Directive.
2. Each Member State would identify the relevant critical infrastructure which satisfy the agreed criteria and notify this list to the Commission at the latest one year after the adoption of the relevant criteria.
3. Within 6 months of the above mentioned identification, the Commission would propose a list of critical infrastructure to be designated as ECI.
4. Within 1 year after designation as ECI each ECI owner/operators would submit its Operator Security Plan to the relevant Member State authority.
5. Within 1 year after designation as ECI each ECI owner/operators would designate its Security Liaison Officer
6. Within 1 year after designation as ECI, each Member State would conduct a risk and threat assessment in relation to that ECI.
7. Within 18 months after designation as ECI, each Member State shall report to the Commission on a summary basis of the types of vulnerabilities, threats and risks encountered in each CIP sector.

Section 8: Monitoring and evaluation

Core indicators of progress

The following achievements could be used to assess progress being made on CIP issues at a horizontal level. Other progress indicators would have to be used in order to assess progress being made in the various sectors (under the sector-by-sector approach).

- Establishment of a CIP contact group composed of representatives of all Member States and relevant Commission services
- Elaboration of common CI sector-based working definitions and terminology
- Creation of an inventory of existing national, bilateral and EU critical infrastructure protection programmes
- Establishment of a list priority sectors/infrastructure that appear most critical at the European level, taking into account interdependencies
- Creation of guidelines on collection and use of sensitive CIP data between Commission, Member States, owners/operators and other relevant parties
- Setting up, where relevant, of CIP sector based expert groups/networks at EU level
- Identification of gaps where Community initiatives would have added-value
- Initiation of EU funding for CIP actions

Possible monitoring and evaluation arrangements

Evaluation and monitoring of the implementation of EPCIP would be a multi-level process requiring the involvement of all stakeholders:

- A peer evaluation mechanism could be established, in which MS and the Commission would work together on assessing the overall level of implementation of EPCIP in each MS.
- The Commission could report progress to MS and other institutions each calendar year in a Commission staff working paper.
- Each Member State could prepare an annual report concerning the overall implementation of EPCIP under its jurisdiction and assessing compliance with its National CIP Programme. These reports would be submitted to the Council and the Commission.

Annex 1: Results of the EPCIP Green Paper – Member State comments

Twenty-two Member States provided official responses to the EPCIP Green Paper consultation process.

The Member States welcomed the Commission's initiative and work on the development of the European Programme for Critical Infrastructure Protection. The national responses to the EPCIP Green Paper supported the fundamental approach of addressing the issue of critical infrastructure protection (CIP) from a European perspective and of developing a European Programme for Critical Infrastructure Protection (EPCIP). The need for increasing the critical infrastructure protection capability in Europe and helping reduce vulnerabilities concerning critical infrastructure was acknowledged. The importance of the principle of subsidiarity was repeatedly stressed in the responses of the Member States.

The EPCIP Green Paper has proved to be a useful instrument in terms of aiding the launch of national discussions concerning critical infrastructure protection.

Goal of EPCIP

The Member States were divided concerning the appropriateness of the goal for EPCIP formulated in the Green Paper. Those Member State which were not satisfied with the presented goal generally emphasised that it is the responsibility of each Member State, and not of a European programme, to guarantee the security of critical infrastructure. Consequently the broad goal of EPCIP should be to raise CIP capability and improve the protection of critical infrastructure in Europe.

Scope of EPCIP

The Member States generally supported the adoption of an all-hazards approach for EPCIP with terrorism being a priority.

Key principles

The Member States generally supported the five key principles listed in the EPCIP Green Paper although a number of modifications and additions were proposed.

Common EPCIP framework

A majority of Member States found that a common EPCIP framework would be an effective tool in strengthening CIP capability in Europe. The Member States were of the opinion that the common framework would be useful in terms of clarifying the responsibilities of the stakeholders concerned. The key role and responsibility of the Member States in this process was repeatedly stressed. The Member States were evenly divided concerning the need for a legislative package for EPCIP. The idea of developing legislation in the future was not ruled out. The Member States were also divided as to the question whether the EPCIP framework should be voluntary or obligatory with a larger number of Member States opting for the obligatory approach.

The Member States generally agreed on the need to have a sector-by-sector approach to the specific provisions of EPCIP. The Member States were generally pleased with the list of critical infrastructure sectors and the list of definitions included in the Green Paper and saw them as a good basis for discussion.

Definition of EU critical infrastructure

The Member States were evenly divided on whether European Critical Infrastructure (ECI) should be defined as infrastructure having a potentially serious cross-border impact on two or more, or three or more Member States. Several Member States emphasised that the definition of ECI should not only be based on the number of Member States affected. The importance of bilateral agreements was also emphasised.

Interdependencies

The importance of identifying interdependencies at various levels was acknowledged by the Member States. Several Member States emphasised the difficulty of this task.

Implementing steps for ECI

The implementing steps concerning ECI were generally seen as useful by a majority of Member States although some responses indicated that it may be too early to clearly define this process. The role of the Commission was generally seen as that of an active participant and facilitator of the EPCIP process.

The NCI role in EPCIP

The Member States were divided concerning the inclusion of NCI in the EPCIP framework. Around half of the Member States saw added value in having EPCIP address NCI at least by way of promoting the exchange of best practices and the building of generic knowledge. Several Member States underlined that EPCIP would have to deal to a certain degree with NCI as it would be infrastructure already designated by a Member State as National Critical Infrastructure which would additionally be designated as European Critical Infrastructure. Around half of the Member States were of the opinion that the best relationship between EPCIP and NCI would be to allow the use of parts of EPCIP as needed in relation to NCI, but that there would be no obligation to do so.

National CIP programmes

The Member States emphasised the need for the development of National CIP Programmes. More than half of the Member States thought that EPCIP could play a positive role in the development of National CIP Programmes either by being the basis for such programmes or inspiring them.

Single overseeing body

All Member States agreed that it is the responsibility of each Member States to designate and manage CI under its jurisdiction. The Member States clearly saw added value in the creation of either a single overseeing body or a single contact point for CIP. Over half of the Member States supported the idea of having a single overseeing/coordination body in each Member State. Several underlined that such bodies already exist.

Implementing steps for NCI

The Member States were generally supportive of the list of implementing steps concerning National Critical Infrastructure proposed in the Green Paper although a number of modifications were proposed.

Responsibilities of CI owners/operators

In general, a majority of Member States found the list of potential responsibilities for CI owners/operators as acceptable. A number of Member States mentioned however the need to

separate the rights/obligations of ECI and NCI. A majority of Member States found the concept of developing Operator Security Plans (OSP) as useful, at the very least, as an example of a best practice. The Member States proposed a number of potential rights which could be given to CI owners/operators.

Dialogue with CI owners/operators

The Member States generally agreed on the need to engage in a public-private dialogue concerning CIP. This dialogue should be conducted at MS level and at EU level on a sector-by-sector basis. At EU level, the private sector should be represented by the relevant industry associations. A number of Member States emphasised the importance of having a voluntary approach to the issue of public-private dialogue. Only through a voluntary partnership, will sufficient levels of trust be built.

Common methodologies

Around half of the Member States saw added value in the idea of harmonizing or calibrating alert levels in the EU and in developing common methodologies of identifying and classifying threats, capabilities, risks, and vulnerabilities and drawing conclusions about the possibility, probability, and degree of severity posed by a threat.

Funding

The Member States did not offer any estimates concerning the costs of implementing the proposals put forward in the EPCIP Green Paper.

Evaluation and monitoring

The Member States generally indicated their support for some form of evaluation mechanism.

Annex 2: Results of the EPCIP Green Paper – comments from industry associations

Nineteen European-level and international industry associations provided comments to the Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP). In addition to a general European business response, a number of industry sectors provided comments:

- Energy sector – responses from five associations
- Transport – responses from seven associations
- IT – responses from two associations
- Water – response from one association
- Chemical - response from one association
- Tank Storage - response from one association
- Security - response from one association

The industry associations generally provided comments on some of the ideas contained in the EPCIP Green Paper, but usually did not respond to the questions posed in the document. Nevertheless a number of messages seemed to be of key concern for them:

- The industry generally supports the creation on an EU-wide EPCIP framework designed to increase the security of critical infrastructure in Europe
- EPCIP must minimize any negative impacts on business competitiveness;
- Duplication of efforts must be avoided;
- The industry underlined the absolute need to be involved from the very outset on the development of EPCIP considering that a majority of critical infrastructure are owned by the private sector;
- A sector-by-sector approach must be pursued in the development of the specific parts of EPCIP;
- Confidentiality is extremely important

The industry associations are generally keen to participate in the dialogue and development of EPCIP.

The transport sector had generally a positive view concerning the EPCIP initiative and the need to address the issue from a European perspective. Nevertheless two of the seven responses, representing a part of the aviation sector and a part of the freight sector, seem to have been provided for the sole purpose of arguing that they should not be covered by anything in EPCIP because they are already contributing to security.

The energy sector underlined the need to conduct a detailed assessment of the situation existing in the energy sector in order to identify gaps and possible solutions. The sector underlined the absolute need for a sectoral approach in addressing CIP issues as several specificities of the sector were mentioned in the responses. The energy sector also emphasised the importance of confidentiality, as public discussions on CIP related issues may increase the vulnerability of certain infrastructure.

The IT and water sectors were generally supportive of the need to improve the security and protection of CIs and expressed their interest in participating in the development of EPCIP.

The chemical sector was also generally supportive but underlined the need to avoid duplication of efforts citing the existence of several instruments which already increase the security and safety of the sector.

The tank storage industry generally felt that its sector should fall outside the remit of EPCIP.

The security industry was generally supportive of the ideas contained in the EPCIP Green Paper and underlined the need for an EU framework addressing CIP issues, based on the experience and expertise of national CIP-efforts.

Goal of EPCIP (question 3.1)

The transport sector provided few concrete comments on this issue. It seems however that the transport industry felt that the goal of EPCIP should be revised. According to one response, the provision of "adequate and equal levels of protective security" is an unrealistic goal considering the differences existing between sectors and the need for effectiveness. One transport association moreover mentioned that EPCIP should facilitate the work of the Member States in the CIP field.

The energy sector did not provide detailed comments on this issue. One response pointed out however that the attainment of "equal levels of protective security" is unrealistic.

The IT sector, water sector and the security industry found the objective identified in the Green Paper as adequate.

The tank storage industry and the chemical industry did not provide comments on this issue.

Scope of EPCIP (question 3.2)

The EPCIP Green Paper posed the question whether EPCIP should be based on an all hazards approach, an all-hazards approach with a terrorism priority or a terrorism hazards approach. The general business view was that EPCIP should have an all-hazards focus, but that it must be sufficiently flexible to deal with the specificities of terrorism.

The transport sector was divided on this issue:

- One response supported the option of basing EPCIP on an all-hazards approach with a terrorism priority;
- One response supported the all-hazards approach
- One response supported the terrorism-hazards approach.

Most of the energy industry would like to restrict the scope of EPCIP to terrorism. This view was expressed in four responses. Two response from the energy sector also emphasised the need to eliminate consequence management from the scope of EPCIP.

The IT sector supported having an all-hazards approach with a terrorism priority. One industry association underlined nevertheless, that if this option is chosen, it must be made clear that other non-terrorist hazards are not put aside.

The security industry would support having an all-hazards approach.

The tank storage industry, water sector and the chemical industry did not provide comments on this issue.

Key principles (question 4)

The EPCIP Green Paper listed five key principles: subsidiarity, complementarity, confidentiality, stakeholder cooperation and proportionality.

The general business position was that it agreed with list of key principles. The principle of confidentiality was stressed as being of crucial importance.

The transport sector generally supported the list of key principles, but suggested a number of slight clarifications.

There was general agreement among the energy related associations on the key principles, but there was particular concern about confidentiality and that any measures should be proportional to risk.

The IT, water, security and tank storage sectors generally supported the list of key principles.

The chemical industry association did not offer comments on this issue.

Common EPCIP framework (question 5)

The EPCIP Green Paper raised several issues concerning the need and format of a potential EPCIP framework in the EU.

The general business position was that an EU EPCIP framework should be established.

The transport sector generally supported an EU approach to identifying ECI through a common framework, including common definitions and principles. However there was no agreement on whether this should be voluntary or mandatory.

The energy sector generally agreed that some form of common framework would be necessary, with those favouring a legislative framework feeling this is needed for setting definitions and responsibilities. No organisation disagreed with the sectoral approach proposed in the Green Paper.

The IT sector supported the idea of having a common EPCIP framework, but was divided on the specific approach to be taken. One response mentioned that if a legislative approach was to be adopted, it should only contain the basic aspects of EPCIP. Another response underlined that the EU framework should be limited to the exchange of best practices.

The tank storage industry supported the idea of a common framework. On the issue of legislation, this industry felt that a step-by-step approach would be preferred with ideas with being tested and then being implemented through legislation.

The security industry supported the idea of having a common framework on CIP. The industry felt that a voluntary approach would be ideal.

The water and chemical industry associations did not offer specific comments on this issue.

The industry generally felt that a framework would be helpful but seemed afraid of overregulation and duplication.

Definition of EU critical infrastructure (question 6.1)

The general business position was that European Critical Infrastructure (ECI) should relate to two or more Member States.

The EU transport industry associations did not provide detailed comments on this. Two responses nevertheless favoured the 2 or more approach.

The energy sector favoured that EPCIP should deal with 3 or more Member States underlining that bilateral agreements should be sufficient to address of CIs.

The IT sector and the security sector supported the 2+ approach.

The water, tank storage and chemical industries did not provide an answer to this issue.

Interdependencies (question 6.2)

The general business position was that interdependencies should be identified at both the national and EU level.

The transport sector did not provide clear comments concerning interdependencies apart from stating that there is no universal approach to the issue and that they are not aware of any concrete methodologies.

The energy sector generally expressed the view that the process of identification of interdependencies should involve all stakeholders and should initially take place at national level.

The IT industry only underlined the need to involve all stakeholders in the process.

The security industry was of the opinion that interdependencies should first be tackled at the national level.

The water, tank storage and chemical industries did not provide an answer to this issue.

Implementing steps for ECI (question 6.3)

The general business position was that the list of implementing steps is fairly complete, but it should also ensure a regular revision of criticality.

The transport sector did not offer concrete comments on whether the list of implementing steps for ECI would be acceptable. Two responses underlined however the need for an arbitration mechanism in case one MS would like to designate a particular infrastructure located in another MS as ECI.

The energy sector was generally supportive of the general implementing steps for ECI contained in the Green Paper.

One response from the IT sector felt that the list of steps was too simple.

The security industry generally supported the list of steps but underlined that private partners should be involved more in the process.

The water, tank storage and chemical industries did not provide an answer to this issue.

The NCI role in EPCIP (question 7.1)

The EPCIP Green Paper raised the issue of what should be the relationship between EPCIP and National Critical Infrastructure.

The general business position was that national critical infrastructure (NCI) should be interrelated with EPCIP in order to ensure the efficiency of the programme.

The transport sector and the energy sector generally considered that national CI should be outside the scope of EPCIP.

The IT sector was divided on this issue with one response recommending that NCI remains outside of EPCIP and a second response feeling that NCI should be addressed by the EPCIP framework, but not by specific regulations.

The tank storage industry felt that EPCIP should not deal with NCI.

The security industry felt that NCI should preferable be integrated in EPCIP.

The water and chemical industries did not provide an answer to this issue.

National CIP programmes (question 7.2)

The EPCIP Green Paper proposed that each Member State develop a National CIP Programme for its NCI based on the common EPCIP framework.

The single response from the transport sector which addressed this issue stated that each Member State should develop such national programmes addressing ECI within the EPCIP framework, and NCI autonomously.

The energy sector seemed to favour basing EPCIP on national programmes rather than national programmes on EPCIP.

The IT sector and the security sector favoured having each Member State adopt a National CIP Programme.

The water, tank storage and chemical industries did not provide an answer to this issue.

Single overseeing body (question 7.3)

The transport sector felt that it should be the Member States who are responsible for designating and managing NCI. The industry also saw added value in having a single coordinating body dealing with CIP issues.

The energy sector and the IT sector generally felt that this issue should be left to each Member State to decide.

The security sector thought that a single coordination body should be created in each Member State.

The water, tank storage and chemical industries did not provide an answer to this issue.

Implementing steps for NCI (question 7.4)

The transport sector did not provide a clear line concerning the implementing steps for NCI. One response reiterated the position that NCI should be outside of EPCIP. Another response felt that the steps were acceptable.

The IT sector limited itself to stating the implementation should be done under the authority of the national CIP body.

The security industry generally supported the list of steps but underlined that private partners should be involved more in the process.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Responsibilities of CI owners/operators(question 8.1)

The general business position was that the list of proposed responsibilities is unclear and may be too burdensome.

The transport sector was divided on this issue. One response clearly stated that the list is acceptable and found the OSP concept useful. Another response underlined that the EPCIP should have at its disposal the necessary financial measure to support the owners/operators.

The energy sector was generally positive about the list of responsibilities although it underlined that the private sector must be involved in discussing this issue.

The IT sector felt that owners/operators should be required to notify the relevant authorities about the fact that they may possess CI.

The security industry offered general comments on this issue.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Dialogue with CI owners/operators(question 8.2)

All industry associations underlined the need for dialogue with CI owners/operators during the development and implementation of EPCIP. Most felt that it should be the associations which represent the relevant sectors in the discussions.

The critical infrastructure warning information network (CIWIN) (question 9.1)

The transport sector supported the idea of creating CIWIN, but different opinions were expressed concerning its structure. One response supported the idea of CIWIN being limited to a rapid-alert network as relevant discussion fora already exist. Another response saw CIWIN as a multilayered communication system composed of two pillars.

The energy sector also supported the idea of CIWIN functioning only as a rapid alert system with the owners/operator being connected to the network.

The IT sector was of the opinion that CIWIN should first become a platform for the exchange of idea and best practices, to later develop into a RAS. Owners/operators should be connected to the system.

The security industry felt that CIWIN should be a 2-pillar system and that owners/operators should also be connected.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Common methodologies (question 9.2)

The single response from transport sector on this issue limited itself to stating that the harmonization of alert levels would be a difficult task.

The energy sector saw added value in harmonizing alert levels but admitted that this would be a very difficult task.

The IT sector and the security industry commented that the development of common methodologies and a harmonization of alert levels would be necessary.

The water, tank storage and chemical industries did not provide a clear view on this issue.

Funding (question 9.3)

The industry associations commenting on this issue underlined that a considerable amount of funding would be needed for EPCIP to be a success. The associations did not provide estimates of the costs involved. Most replies were positive concerning the availability of funds for research purposes.

Evaluation and monitoring (question 9.3)

Most industry associations commenting on this issue felt that some sort of evaluation mechanism would be needed. The transport sector generally accepted the proposed methods. One response from the energy sector expressed concern over the possibility of imposing penalties.

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 12.12.2006
KOM(2006) 786 lopullinen

TIEDONANTO

Elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta

TIEDONANTO

Elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta

(ETA:n kannalta merkityksellinen teksti)

1. TAUSTAA

Kesäkuussa 2004 kokoontunut Eurooppa-neuvosto pyysi komissiota laatimaan kokonaisstrategian elintärkeiden infrastruktuurien suojaamiseksi. Komissio hyväksyi tämän vuoksi 20. lokakuuta 2004 tiedonannon ”Kriittisen infrastruktuurin suojelu terrorismin torjunnassa”. Tiedonannossa esitetään, miten Euroopassa voitaisiin entistä paremmin ehkäistä elintärkeisiin infrastruktuureihin kohdistuvia terrori-iskuja sekä varautua ja reagoida niihin.

Neuvosto hyväksyi joulukuussa 2004 terrori-iskujen ehkäisemistä, niihin varautumista ja niihin reagoimista koskevat päätelmät sekä terroriuhkien ja -iskujen seurauksia koskevan EU:n yhteisvastuuohjelman. Samalla se antoi hyväksyntänsä komission aikomukselle esittää elintärkeiden infrastruktuurien suojaamista koskeva EU:n ohjelma (European Programme for Critical Infrastructure Protection, EPCIP) ja perustaa elintärkeiden infrastruktuurien varoitusjärjestelmä (Critical Infrastructure Warning Information Network, CIWIN).

Marraskuussa 2005 komissio hyväksyi vihreän kirjan Euroopan elintärkeiden infrastruktuurien suojaamisohjelmasta. Siinä esitetään vaihtoehtoja suojaamisohjelman ja varoitusjärjestelmän toteuttamista varten.

Joulukuussa 2005 kokoontunut oikeus- ja sisäasioiden neuvosto kehotti elintärkeiden infrastruktuurien suojaamista koskevissa päätelmissään komissiota laatimaan ehdotuksen elintärkeiden infrastruktuurien suojaamista koskevaksi EU:n ohjelmaksi.

Tässä tiedonannossa esitellään elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttamista varten ehdotetut periaatteet, menettelyt ja välineet. Suojaamisohjelman toteuttamista tuetaan tarvittaessa alakohtaisin tiedonannoin, joissa esitetään komission lähestymistapa elintärkeiden infrastruktuurien eri aloilla[1].

2. ELINTÄRKEIDEN INFRASTRUKTUURIEN SUOJAAMISTA KOSKEVAN EU:N OHJELMAN TARKOITUS, PERIAATTEET JA SISÄLTÖ

2.1. Ohjelman tavoite

Ohjelman yleistavoitteena on parantaa elintärkeiden infrastruktuurien suojaamista Euroopan unionissa. Tavoite saavutetaan perustamalla elintärkeiden infrastruktuurien suojaamista koskeva EU:n kehys. Kehys esitellään tässä tiedonannossa.

[1] Komissio aikoo esittää tiedonannon Euroopan elintärkeiden energia- ja liikenneinfrastruktuurien suojaamisesta.

2.2. Millaisia uhkia ohjelman avulla on tarkoitus ehkäistä?

Vaikka elintärkeisiin infrastruktuureihin kohdistuvana ensisijaisena uhkana pidetäänkin terrorismia, suojaamistoimissa on tarkoitus ottaa huomioon kaikki vaaratekijät. Jos todetaan, että suojaamistoimenpiteet ovat jollakin tietyllä toimialalla riittävällä tasolla, sidosryhmien tulisi keskittyä niihin uhkiin, joille ne ovat edelleen alttiina.

2.3. Periaatteet

Ohjelman toteuttaminen perustuu seuraaviin periaatteisiin:

- **Toissijaisuus** – Komission toiminta keskittyy sellaisten infrastruktuurien suojaamiseen, jotka ovat elintärkeitä nimenomaan koko Euroopan kannalta eivätkä vain kansallisesta tai alueellisesta näkökulmasta. Tästä painopisteestä huolimatta komissio voi voimassa olevat yhteisön toimivaltuudet ja käytettävissä olevat resurssit huomioon ottaen tukea jäsenvaltioita niiden pyynnöstä myös kansallisesti elintärkeiden infrastruktuurien suojaamisessa.

- **Täydentävyys** – Komissio pyrkii välttämään päällekkäisiä toimia silloin kun EU:n tasolla tai kansallisella tai alueellisella tasolla on jo toteutettu toimia, jotka ovat osoittautuneet tehokkaiksi elintärkeiden infrastruktuurien suojaamisessa. Ohjelma onkin tarkoitus laatia jo olemassa olevien alakohtaisten toimien pohjalta täydentämällä niitä.

- **Luottamuksellisuus** – Elintärkeiden infrastruktuurien suojaamiseen liittyvät tiedot luokitellaan salaisiksi sekä EU:n että jäsenvaltioiden tasolla, ja tietoihin saavat tutustua ainoastaan ne, jotka niitä todella tarvitsevat. Elintärkeitä infrastruktuureja koskevan tietojenvaihdon tulisi tapahtua luottamuksellisesti ja suojatussa ympäristössä.

- **Yhteistyö sidosryhmien kanssa** – Kaikki sidosryhmät otetaan mahdollisimman laajalti mukaan suojaamisohjelman kehittämiseen ja toteuttamiseen. Tämä tarkoittaa sekä Euroopan elintärkeiksi infrastruktuureiksi nimettyjen infrastruktuurien omistajia/ylläpitäjiä että julkisia viranomaisia ja muita asianomaisia elimiä.

- **Oikeasuhteisuus** – Toimenpiteitä ehdotetaan toteutettavaksi vain silloin kun ne on todettu tarpeellisiksi nykyisten turvallisuusvajeiden perusteella. Toimenpiteiden on oltava oikeassa suhteessa asianomaisen vaaran tai uhkan tasoon ja tyyppiin.

- **Alakohtainen lähestymistapa** – Koska eri toimialoilla on kertynyt erityistä kokemusta ja asiantuntemusta elintärkeiden infrastruktuurien turvaamisesta ja ne asettavat myös omat vaatimuksensa tälle toiminnalle, suojaamisohjelmassa noudatetaan alakohtaista lähestymistapaa, ja sitä toteutetaan elintärkeiden infrastruktuurien suojaamisen eri aloja koskevan yhteisen luettelon pohjalta.

2.4. Suojaamisohjelman toimintakehys

Elintärkeiden infrastruktuurien suojaamisohjelman toimintakehys käsittää seuraavat tekijät:

- Menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteinen lähestymistapa niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten. Nämä toimet toteutetaan antamalla direktiivi.

- Toimet, joiden tarkoituksena on helpottaa elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttamista: mm. suojaamisohjelman toteuttamista koskeva toimintasuunnitelma, elintärkeiden infrastruktuurien varoitusjärjestelmä (CIWIN), elintärkeiden infrastruktuurien suojaamista käsittelevät EU:n tason asiantuntijaryhmät, elintärkeiden infrastruktuurien suojaamista koskevaan tietojenvaihtoon liittyvät menettelyt sekä infrastruktuurien keskinäisten riippuvuussuhteiden määrittäminen ja analysointi.

- Jäsenvaltioiden tukeminen kansallisten elintärkeiden infrastruktuurien suojaamisessa asianomaisten jäsenvaltioiden pyynnöstä. Tässä tiedonannossa esitetään kansallisten elintärkeiden infrastruktuurien suojaamista koskevat perussuuntaviivat.

- Valmiussuunnitelmat

- Toiminnan ulkoinen ulottuvuus

- Toimintaan liittyvät rahoitustoimet ja erityisesti ehdotus terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa koskevaksi erityisohjelmaksi kaudelle 2007–2013. Erityisohjelmasta voidaan rahoittaa elintärkeiden infrastruktuurien suojaamiseen liittyviä toimia, joita voidaan hyödyntää useissa EU:n jäsenvaltioissa.

Näitä toimenpiteitä esitellään lähemmin jäljempänä.

2.5. Elintärkeän infrastruktuurin suojaamisesta vastaavien yhteyspisteiden ryhmä

Tarvitaan EU:n tason mekanismi, joka vastaa strategisesta koordinoinnista ja yhteistyöstä ja jolla on valmiudet suunnitella elintärkeiden infrastruktuurien suojaamista koskevaan EU:n ohjelmaan liittyviä yleisiä ja alakohtaisia toimia. Tätä varten perustetaan elintärkeiden infrastruktuurien suojaamisesta vastaavien yhteyspisteiden ryhmä.

Ryhmän muodostavat kunkin jäsenvaltion elintärkeiden infrastruktuurien suojaamisesta vastaavat yhteyspisteet. Ryhmän puheenjohtajana toimii komissio. Jokaisen jäsenvaltion on nimettävä elintärkeiden infrastruktuurien suojaamisesta vastaava yhteyspiste, jonka tehtävänä on koordinoida tähän liittyviä kysymyksiä sekä jäsenvaltion sisällä että muiden jäsenvaltioiden, neuvoston ja komission kanssa. Tällaisen yhteyspisteen nimeäminen ei estä jäsenvaltion muita viranomaisia osallistumasta elintärkeiden infrastruktuurien suojaamiseen.

3. EUROOPAN ELINTÄRKEÄT INFRASTRUKTUURIT (EEI)

Euroopan elintärkeillä infrastruktuureilla tarkoitetaan yhteisön kannalta tärkeimpiä infrastruktuureja, joiden vahingoittuminen tai tuhoutuminen aiheuttaisi seurauksia kahdessa tai useammassa jäsenvaltiossa tai vain yhdessä jäsenvaltiossa siinä tapauksessa, että infrastruktuuri ei sijaitse kyseisessä jäsenvaltiossa. Tähän voi liittyä valtioiden rajat ylittäviä seurauksia, jotka johtuvat toisiinsa liitettyjen, eri alojen infrastruktuurien keskinäisistä riippuvuussuhteista. Menettely Euroopan elintärkeiden infrastruktuurien määrittämistä ja nimeämistä varten sekä yhteinen lähestymistapa niiden suojaamisen parantamiseen liittyvien tarpeiden arvioimista varten otetaan käyttöön antamalla asiaa koskeva direktiivi.

4. SUOJAAMISOHJELMAN LAATIMISTA JA TOTEUTTAMISTA HELPOTTAVAT TOIMENPITEET

Komissio toteuttaa eri toimenpiteitä helpottaakseen elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttamista ja muuta elintärkeiden infrastruktuurien suojaamiseen liittyvää toimintaa EU:n tasolla.

4.1. Suojaamisohjelmaa koskeva toimintasuunnitelma

Elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttaminen on jatkuva prosessi, jota tarkastellaan säännöllisesti erityisen toimintasuunnitelman avulla. Toimintasuunnitelmaan kirjataan toteutettavat toimet ja niiden aikataulu. Toimintasuunnitelmaa (liite) päivitetään säännöllisesti sitä mukaa kun sen täytäntöönpano etenee.

Suojaamisohjelman toimet jaetaan toimintasuunnitelmassa kolmeen toimintalinjaan:

- toimintalinja 1 koskee suojaamisohjelman strategisia näkökohtia ja elintärkeiden infrastruktuurien suojaamiseksi toteutettavien horisontaalisten toimien suunnittelua;
- toimintalinja 2 koskee Euroopan elintärkeitä infrastruktuureja alakohtaisella tasolla;
- toimintalinja 3 koskee jäsenvaltioiden tukemista kansallisten elintärkeiden infrastruktuurien suojaamisessa.

Suojaamisohjelmaa koskevan toimintasuunnitelman toteuttamisessa otetaan huomioon alakohtaiset erityisvaatimukset ja tarvittaessa myös muut sidosryhmät.

4.2. Elintärkeiden infrastruktuurien varoitusjärjestelmä (CIWIN)

Elintärkeiden infrastruktuurien varoitusjärjestelmä (Critical Infrastructure Warning Information Network, CIWIN) perustetaan erillisellä komission ehdotuksella päällekkäisiä toimia välttäen. Varoitusjärjestelmän avulla on tarkoitus vaihtaa parhaita käytäntöjä suojatussa ympäristössä. CIWIN täydentää jo käytössä olevia verkostoja. Komission Argus-järjestelmään liitettynä sitä voitaisiin myös käyttää kiireellisten varoitusten välittämiseen. Varoitusjärjestelmän turvallisuusjärjestelyt toteutetaan tarvittavien menettelyjen mukaisesti.

4.3. Asiantuntijaryhmät

Vuoropuhelu sidosryhmien kanssa on olennaisen tärkeää, kun halutaan parantaa EU:n elintärkeiden infrastruktuurien suojaamista. Saadakseen tarvittaessa käyttöönsä erityisasiantuntemusta komissio voi perustaa asiantuntijaryhmiä, jotka käsittelevät elintärkeiden infrastruktuurien suojaamiseen liittyviä erityiskysymyksiä ja edistävät tähän liittyvää julkisen ja yksityisen sektorin välistä vuoropuhelua. Asiantuntijaryhmät tukevat suojaamisohjelman toteuttamista, sillä niiden puitteissa asiantuntijat voivat vaihtaa näkemyksiä ja antaa neuvoja elintärkeiden infrastruktuurien suojaamiseen liittyvistä kysymyksistä. Asiantuntijaryhmien toiminta perustuu vapaaehtoisuuteen. Siinä yhdistetään julkisen ja yksityisen sektorin resurssit, niin että voidaan saavuttaa jokin tietty tavoite tai useampia tavoitteita, joista katsotaan olevan etua sekä kansalaisille että yksityiselle sektorille.

Nämä asiantuntijaryhmät eivät korvaa mitään aiemmin perustettuja ryhmiä, eikä minkään jo toimivan ryhmän toimeksiantoa ole tarkoitus mukauttaa suojaamisohjelman tarpeisiin.

Asiantuntijaryhmät eivät myöskään osallistu teollisuuden, jäsenvaltioiden viranomaisten ja komission väliseen suoraan tietojenvaihtoon.

Elintärkeiden infrastruktuurien suojaamista käsittelevälle EU:n asiantuntijaryhmälle annetaan selkeästi määritelty tavoite ja aikataulu sen saavuttamista varten. Myös jäsenten profiili määritellään selkeästi. Kun asiantuntijaryhmät ovat saavuttaneet tavoitteensa, ne lakkautetaan.

Asiantuntijaryhmien erityistehtävät voivat vaihdella kunkin elintärkeään infrastruktuuriin kuuluvan alan ominaispiirteiden mukaan. Asiantuntijaryhmille voidaan antaa mm. seuraavia tehtäviä:

- infrastruktuurien heikkouksien ja keskinäisten riippuvuussuhteiden sekä alakohtaisten parhaiden käytänteiden määrittäminen;
- merkittävien heikkouksien vähentämiseen ja/tai poistamiseen tähtäävien toimenpiteiden ja suorituskyvyn mittaamisen suunnittelu;
- elintärkeiden infrastruktuurien suojaamiseen liittyvän tietojenvaihdon, koulutuksen ja luottamuksen lisääminen;
- erilaisten liiketoimintaratkaisujen (*business case*) suunnittelu ja niistä tiedottaminen eri aloilla, jotta alan toimijoille voidaan osoittaa, mitä hyötyä infrastruktuurien suojaamista koskevien suunnitelmien laatimiseen ja muihin suojaamiseen tähtääviin aloitteisiin osallistumisesta voi olla;
- alakohtaisen asiantuntija-avun ja neuvojen antaminen esimerkiksi tutkimukseen ja kehittämiseen liittyvissä kysymyksissä.

4.4. Elintärkeiden infrastruktuurien suojaamiseen liittyvä tietojenvaihto

Elintärkeiden infrastruktuurien suojaamiseen liittyvä tietojenvaihto sidosryhmien kesken edellyttää keskinäistä luottamusta, niin että vapaaehtoisesti luovutetut liikesalaisuudet tai muutoin arkaluonteiset tai henkilökohtaiset tiedot eivät päädy julkisuuteen, vaan että arkaluonteiset tiedot suojataan asianmukaisella tavalla. Myös oikeutta yksityisyydensuojaan on kunnioitettava.

Sidosryhmien on toteutettava tarvittavat toimenpiteet, jotta tiedot voidaan suojata asianmukaisella tavalla. Suojattavia tietoja ovat tiedot elintärkeiden infrastruktuurien ja suojattujen järjestelmien turvallisuudesta, keskinäisiä riippuvuussuhteita koskevat selvitykset ja arviot elintärkeiden infrastruktuurien haavoittuvuudesta sekä niihin kohdistuvista uhkista ja riskeistä. Tällaisia tietoja on käytettävä ainoastaan elintärkeiden infrastruktuurien suojaamiseen. Jokaisesta luottamuksellisia tietoja käsittelevästä henkilöstä on laadittava asianmukainen turvallisuusselvitys siinä jäsenvaltiossa, jonka kansalainen hän on.

Elintärkeiden infrastruktuurien suojaamista koskevassa tietojenvaihdossa on otettava huomioon myös se, että määrätyt tiedot voivat olla arkaluonteisia siitä huolimatta, että niillä ei ole turvaluokitusta.

Elintärkeiden infrastruktuurien suojaamista koskeva tietojenvaihto tukee seuraavia tavoitteita:

- entistä tarkempien tietojen saaminen ja ymmärtämyksen lisääminen infrastruktuurien keskinäisistä riippuvuussuhteista, niihin kohdistuvista uhkista, niiden heikkouksista, turvavälikohtauksista, vastatoimenpiteistä ja elintärkeiden infrastruktuurien suojaamiseen liittyvistä parhaista käytänteistä;

- tietoisuuden lisääminen elintärkeisiin infrastruktuureihin liittyvistä näkökohdista;

- sidosryhmien välinen vuoropuhelu;

- koulutuksen, tutkimuksen ja kehittämisen tarkempi kohdentaminen.

4.5. Keskinäisten riippuvuussuhteiden määrittäminen

Sekä maantieteellisten että eri alojen keskinäisten riippuvuussuhteiden selvittäminen ja analysointi on erittäin tärkeä tehtävä, kun halutaan parantaa elintärkeiden infrastruktuurien suojaamista Euroopan unionissa. Tämä jatkuva prosessi on otettava huomioon, kun arvioidaan EU:n alueella sijaitsevien elintärkeiden infrastruktuurien heikkouksia ja niihin kohdistuvia uhkia ja riskejä.

5. KANSALLISET ELINTÄRKEÄT INFRASTRUKTUURIT

Yhteisön voimassa olevien toimivaltuuksien mukaan vastuu kansallisten elintärkeiden infrastruktuurien suojaamisesta kuuluu niiden omistajille/ylläpitäjille ja jäsenvaltioille. Komissio voi kuitenkin tukea jäsenvaltioita tässä työssä, jos ne sitä pyytävät.

Kaikkia jäsenvaltioita kehotetaan parantamaan kansallisten elintärkeiden infrastruktuurien suojaamista laatimalla tätä varten erityinen ohjelma. Tällaisten ohjelmien tavoitteena olisi määrittää kunkin jäsenvaltion lähestymistapa sen alueella sijaitsevien kansallisten elintärkeiden infrastruktuurien suojaamiseen. Ohjelmissa olisi käsiteltävä ainakin seuraavia kysymyksiä:

- Kansallisten elintärkeiden infrastruktuurien määrittäminen ja nimeäminen kansallisten kriteerien perusteella. Jokaisen jäsenvaltion olisi laadittava tällaiset kriteerit siten, että niissä otetaan huomioon ainakin seuraavat laadulliset ja määrälliset seuraukset, joita tietyn infrastruktuurin vahingoittuminen tai tuhoutuminen voisi aiheuttaa:

  - Laajuus - Tietyn elintärkeän infrastruktuurin vahingoittumisen tai tuhoutumisen laajuutta arvioidaan määrittelemällä maantieteellinen alue, johon infrastruktuurin menetyksen seuraukset vaikuttaisivat.

  - Vakavuus - Tietyn infrastruktuurin vahingoittumisen tai tuhoutumisen aiheuttamien seurausten vakavuutta olisi arvioitava seuraavien kriteerien nojalla:

  – vaikutukset väestöön (kohteena olevan väestön määrä);

  – taloudelliset vaikutukset (taloudellisten menetysten ja/tai tuotteiden tai palvelujen laadun heikkenemisen suuruusluokka);

– ympäristövaikutukset;

– poliittiset vaikutukset;

– psykologiset vaikutukset;

– kansanterveyteen liittyvät vaikutukset.

Jos jossakin jäsenvaltiossa ei ole määritelty tällaisia kriteereitä, komissio voi jäsenvaltion pyynnöstä avustaa sitä tarjoamalla sen käyttöön tarvittavat menetelmät.

- Vuoropuhelun käynnistäminen elintärkeiden infrastruktuurien omistajien/ylläpitäjien kesken.

- Maantieteellisten ja eri alojen keskinäisten riippuvuussuhteiden määrittäminen.

- Kansallisia elintärkeitä infrastruktuureja koskevien valmiussuunnitelmien laatiminen (tarvittaessa).

- Jäsenvaltioita kannustetaan laatimaan kansallisten elintärkeiden infrastruktuurien suojaamista koskevat ohjelmansa Euroopan elintärkeiden infrastruktuurien määrittämistä varten laaditun, elintärkeän infrastruktuurin eri aloja koskevan yhteisen luettelon pohjalta.

Jos jäsenvaltiot noudattavat kansallisten elintärkeiden infrastruktuurien suojaamisessa samoja periaatteita, on helpompi varmistaa, että elintärkeiden infrastruktuurien sidosryhmät eri puolilla Eurooppaa voivat hyötyä siitä, että niiden ei tarvitse noudattaa monia erilaisia toimintaperiaatteita, mistä aiheutuisi ylimääräisiä kustannuksia. Näin voidaan myös varmistaa, että kilpailu sisämarkkinoilla ei vääristy.

6. VALMIUSSUUNNITTELU

Valmiussuunnittelu on elintärkeiden infrastruktuurien suojaamisen keskeinen osa-alue, jonka tarkoituksena on minimoida elintärkeän infrastruktuurin vahingoittumisesta tai tuhoutumisesta aiheutuvat seuraukset. Valmiussuunnitelmia koskevan johdonmukaisen lähestymistavan muotoilun tulisi olla keskeinen osa elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman toteuttamista. Valmiussuunnitelmissa olisi käsiteltävä mm. elintärkeiden infrastruktuurien omistajien/ylläpitäjien osallistumista, yhteistyötä kansallisten viranomaisten kanssa ja tietojenvaihtoa naapurimaiden kanssa.

7. ULKOINEN ULOTTUVUUS

Terrorismi ja muu rikollisuus, luonnonkatastrofit ja muut onnettomuuksien syyt eivät tunnusta valtioiden rajoja. Uhkatekijöitä ei voida tarkastella yksinomaan kansallisesta näkökulmasta. Siksi elintärkeiden infrastruktuurien suojaamisohjelman toteuttamisessa on otettava täysimääräisesti huomioon suojaamistoimien ulkoinen ulottuvuus. Koska nykypäivän talous- ja yhteiskuntaelämälle ovat ominaisia monenlaiset yhteysverkostot ja riippuvuussuhteet, myös EU:n ulkopuolella ilmenevät häiriöt saattavat aiheuttaa vakavia seurauksia yhteisölle ja sen jäsenvaltioille. Vastaavasti jonkin EU:n alueella sijaitsevan elintärkeän infrastruktuurin vahingoittuminen tai tuhoutuminen voi aiheuttaa vahinkoa EU:n kumppanimaissa. On myös otettava huomioon, että pyrkimällä parantamaan elintärkeiden infrastruktuurien suojaamista EU:n alueella voidaan samalla vähentää EU:n talouselämälle aiheutuvia häiriöitä ja edistää siten EU:n maailmanlaajuista taloudellista kilpailukykyä.

Elintärkeiden infrastruktuurien suojaamisohjelmassa olisi tämän vuoksi kiinnitettävä erityistä huomiota suojaamiseen liittyvän yhteistyön tehostamiseen myös EU:n ulkopuolella esimerkiksi alakohtaisten yhteisymmärryspöytäkirjojen avulla (niissä voitaisiin käsitellä mm. yhteisiä standardeja, elintärkeiden infrastruktuurien suojaamista käsittelevien yhteisten selvitysten laatimista sekä yhteisten uhkakuvien määrittämistä ja suojaamistoimiin liittyvien parhaiden käytänteiden vaihtoa). Lisäksi olisi pyrittävä parantamaan elintärkeiden infrastruktuurien suojaamiseen liittyviä standardeja myös EU:n ulkopuolella. Elintärkeiden infrastruktuurien suojaamiseen liittyvässä yhteistyössä keskitytään EU:n naapurimaihin. Tietyillä aloilla, kuten tietotekniikan ja rahoituksen alalla, tarvitaan kuitenkin laaja-alaisempaa lähestymistapaa, koska niiden toiminta perustuu maailmanlaajuisten järjestelmien keskinäisiin yhteyksiin. Vuoropuheluun ja parhaiden käytänteiden vaihtoon olisi saatava mukaan kaikki EU:n yhteistyökumppanit ja kansainväliset organisaatiot. Komissio pyrkii myös edelleen kehittämään elintärkeiden infrastruktuurien suojaamista EU:n ulkopuolisissa maissa tekemällä yhteistyötä G8- ja Euro–Välimeri-kumppanuusmaiden sekä naapuruuspolitiikan piiriin kuuluvien maiden kanssa jo käytössä olevien rakenteiden ja politiikkojen, kuten vakausvälineen, avulla.

8. TOIMINNAN RAHOITUS

Elintärkeiden infrastruktuurien suojaamista koskevan EU:n ohjelman täytäntöönpanoa edistää osaltaan terrorismin ja muiden turvallisuusriskien ehkäisemistä, torjuntavalmiutta ja seurausten hallintaa koskeva erityisohjelma, jota on määrä toteuttaa vuosina 2007–2013.

Tämän erityisohjelman yleisiin tavoitteisiin kuuluu tukea, edistää ja kehittää kaikenlaisten turvallisuusriskien ja erityisesti terrori-iskujen ehkäisemiseen tai vähentämiseen, niihin varautumiseen ja niiden seurausten hallintaan tähtääviä toimenpiteitä, tarvittaessa uhkia ja riskejä koskevien kattavien arviointien avulla ja siinä määrin kuin tällaista toimintaa ei tueta muista rahoitusvälineistä.

Erityisohjelman perusteella myönnetään tukea avustusten ja komission aloitteesta toteutettavien toimien muodossa. Tuen avulla on tarkoitus mm. suunnitella erilaisia välineitä, strategioita, menetelmiä, selvityksiä, arviointeja ja toteuttaa toimia ja toimenpiteitä elintärkeiden infrastruktuurien tehokkaan suojaamisen varmistamiseksi (sekä EU:n että jäsenvaltioiden tasolla).

LIITE

Elintärkeiden infrastruktuurien suojaamista koskevaan EU:n ohjelmaan liittyvä toimintasuunnitelma

Toimintalinja 1. Suojaamisohjelmaa koskevat strategiat

Toimintalinja 1 muodostaa strategisen perustan koko suojaamisohjelman puitteissa tarvittavalle koordinoinnille ja yhteistyölle, joka on elintärkeiden infrastruktuurien suojaamisesta vastaavien yhteyspisteiden ryhmän tehtävä.

1. vaihe

Toimi	Toimija	Aikataulu
määritetään painopistealat (ensisijaisia painopistealoja ovat liikenne ja energia)	komissio	mahdollisimman pian ja sen jälkeen vuosittain
laaditaan elintärkeitä infrastruktuureja koskevia alakohtaisia työmääritelmiä ja terminologiaa	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	viimeistään vuosi Euroopan elintärkeitä infrastruktuureja (EEI) koskevan direktiivin voimaantulon jälkeen
laaditaan Euroopan elintärkeiden infrastruktuurien (EEI) määrittämisessä käytettävät yleiset kriteerit	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	viimeistään vuosi EEI-direktiivin voimaantulon jälkeen
luetteloidaan elintärkeiden infrastruktuurien suojaamista koskevat nykyiset kansalliset, kahdenväliset ja EU:n tason ohjelmat	komissio, jäsenvaltiot	vireillä
laaditaan arkaluonteisten tietojen keräämistä ja käyttöä koskevat sidosryhmien yhteiset suuntaviivat	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	vireillä
kerätään elintärkeiden infrastruktuurien suojaamiseen liittyviä parhaita käytänteitä, riskinarviointivälineitä ja menetelmiä	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	vireillä
tilataan selvityksiä infrastruktuurien keskinäisistä riippuvuussuhteista	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	vireillä

2. vaihe

Toimi	Toimija	Aikataulu
määritetään ne nykyisissä toimissa ilmenevät puutteet, joiden korjaamiseen yhteisön toimet voisivat tuoda lisäarvoa	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	vireillä
perustetaan elintärkeiden infrastruktuurien suojaamista koskevia alakohtaisia EU:n tason asiantuntijaryhmiä (tarvittaessa)	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	vireillä
selvitetään, millaisia elintärkeiden infrastruktuurien suojaamistoimia voidaan rahoittaa EU:n varoin	komissio, jäsenvaltiot	vireillä
tehdään aloite EU:n rahoituksen myöntämisestä elintärkeiden infrastruktuurien suojaamiseen	komissio	vireillä

3. vaihe

Toimi	Toimija	Aikataulu
valmistellaan yhteistyötä kolmansien maiden ja kansainvälisten organisaatioiden kanssa	komissio, jäsenvaltiot	vireillä

Toimintalinja 2. Euroopan elintärkeiden infrastruktuurien (EEI) suojaaminen

Toimintalinja 2 tähtää ensisijaisesti EEI:n haavoittuvuuden vähentämiseen.

1. vaihe

Toimi	Toimija	Aikataulu
laaditaan EEI:n määrittämisessä käytettävät alakohtaiset kriteerit	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	viimeistään vuosi EEI-direktiivin voimaantulon jälkeen

2. vaihe

Toimi	Toimija	Aikataulu
määritetään ja tarkistetaan alakohtaisesti, mitkä infrastruktuurit olisi todettava koko Euroopan kannalta elintärkeiksi infrastruktuureiksi	komissio, jäsenvaltiot	viimeistään vuoden kuluttua kriteerien hyväksymisestä ja sen jälkeen jatkuvasti
nimetään Euroopan elintärkeät infrastruktuurit	komissio, jäsenvaltiot	vireillä

määritetään EEI:n eri osien heikkoudet ja niihin kohdistuvat uhkat ja riskit sekä laaditaan turvallisuussuunnitelmat	komissio, jäsenvaltiot, EEI:n omistajat/ylläpitäjät (yleinen raportti komissiolle)	viimeistään vuoden kuluttua EEI:n nimeämisestä
kartoitetaan suojaamistoimien ja erityisesti EU:n tason toimien tarve	komissio, jäsenvaltiot ja tarvittaessa muut sidosryhmät	viimeistään 1,5 vuoden kuluttua EEI:n nimeämisestä
kartoitetaan eri jäsenvaltioissa sovellettavat EEI:n hälytystasot laaditaan toteutettavuustutkimus hälytystasojen kalibroinnista tai yhtenäistämisestä	komissio, jäsenvaltiot	vireillä

3. vaihe

Toimi	Toimija	Aikataulu
laaditaan ja hyväksytään ehdotuksia EEI:n suojaamista koskevista vähimmäistoimista	komissio, jäsenvaltiot, EEI:n omistajat/ylläpitäjät	kun suojaamistoimien ja erityisesti EU:n tason toimien tarve on kartoitettu
toteutetaan suojaamista koskevat vähimmäistoimet	jäsenvaltiot, EEI:n omistajat/ylläpitäjät	vireillä

Toimintalinja 3. Kansallisiin elintärkeisiin infrastruktuureihin liittyvät tukitoimet

Toimintalinja 3 on jäsenvaltioiden sisäinen toimintalinja, jonka tarkoituksena on tukea jäsenvaltioita kansallisten elintärkeiden infrastruktuurien suojaamisessa.

1. vaihe

Toimi	Toimija	Aikataulu
vaihdetaan tietoja kansallisten elintärkeiden infrastruktuurien määrittämisessä käytettävistä kriteereistä	jäsenvaltio (komissio voi tarvittaessa avustaa)	vireillä

2. vaihe

Toimi	Toimija	Aikataulu
määritetään ja tarkistetaan alakohtaisesti, mitkä infrastruktuurit olisi todettava kansallisesti elintärkeiksi infrastruktuureiksi	jäsenvaltio ja tarvittaessa muut sidosryhmät	vireillä

nimetään tietyt infrastruktuurit kansallisesti elintärkeiksi infrastruktuureiksi	jäsenvaltio	vireillä
kartoitetaan alakohtaisesti kansallisten elintärkeiden infrastruktuurien turvallisuusvajeet	jäsenvaltiot ja tarvittaessa muut sidosryhmät (komissio voi tarvittaessa avustaa)	vireillä

3. vaihe

Toimi	Toimija	Aikataulu
laaditaan ja kehitetään kansallisten elintärkeiden infrastruktuurien suojaamisohjelmia	jäsenvaltio (komissio voi tarvittaessa avustaa)	vireillä
suunnitellaan erityisiä suojaamistoimia kutakin kansallista elintärkeää infrastruktuuria varten	jäsenvaltio, kansallisen elintärkeän infrastruktuurin omistaja/ylläpitäjä (komissio voi tarvittaessa avustaa)	vireillä
valvotaan, että infrastruktuurien omistajat/ylläpitäjät toteuttavat tarvittavat toimet	jäsenvaltio	vireillä

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 12.12.2006
KOM(2006) 786 slutlig

MEDDELANDE FRÅN KOMMISSIONEN

om ett europeiskt program för skydd av kritisk infrastruktur

MEDDELANDE FRÅN KOMMISSIONEN

om ett europeiskt program för skydd av kritisk infrastruktur

(Text av betydelse för EES)

1. BAKGRUND

Vid sitt möte i juni 2004 efterlyste Europeiska rådet en övergripande strategi för skydd av kritisk infrastruktur. Den 20 oktober 2004 antog kommissionen ett meddelande om kritisk infrastruktur i kampen mot terrorismen, med tydliga förslag om vad som skulle kunna förbättra de förebyggande åtgärderna, beredskapen och insatserna i Europa mot terroristattacker som drabbar kritisk infrastruktur.

I rådets slutsatser om att förebygga, ha beredskap för och bemöta terroristattacker samt i EU:s solidaritetsprogram om konsekvenserna av terrorisThot och terroristattacker, som antogs av rådet i december 2004, godkändes kommissionens planer på att föreslå ett europeiskt program för skydd av kritisk infrastruktur (EPCIP). Vidare samtyckte rådet till att kommissionen inrättar ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN).

I november 2005 antog kommissionen en grönbok om ett europeiskt program för skydd av kritisk infrastruktur (EPCIP), som anger hur kommissionen skulle kunna gå till väga för att inrätta ett europeiskt program för skydd av kritisk infrastruktur och ett nätverk för varningar om hot mot kritisk infrastruktur.

I sina slutsatser från december 2005 om skydd av kritisk infrastruktur uppmanade rådet (rättsliga och inrikes frågor) kommissionen att lägga fram ett förslag till europeiskt program för skydd av kritisk infrastruktur.

Det här meddelandet tar upp de principer, processer och instrument som föreslås för att genomföra det europeiska programmet för skydd av kritisk infrastruktur. Genomförandet av EPCIP kommer i relevanta fall att ledsagas av sektorsspecifika meddelanden som redovisar kommissionens syn när det gäller enskilda sektorer med kritisk infrastruktur[1].

2. ETT EUROPEISKT PROGRAM FÖR SKYDD AV KRITISK INFRASTRUKTUR: SYFTE, PRINCIPER OCH INNEHÅLL

2.1. Syftet med EPCIP

Det allmänna målet med det europeiska programmet för skydd av kritisk infrastruktur är att förbättra skyddet av kritisk infrastruktur i EU. Detta mål kommer att kunna uppnås genom inrättande av en sådan EU-ram för skyddet av kritisk infrastruktur som beskrivs i detta meddelande.

---

[1] Kommissionen avser att lägga fram ett meddelande om skydd av kritisk energi- och transportinfrastruktur i EU.

2.2. Vad bör EPCIP skydda mot

Samtidigt som hotet från terrorismen är en prioritering kommer skyddet av kritisk infrastruktur att bygga på en strategi som omfattar alla relevanta risker. Om skyddsåtgärderna inom en viss sektor av kritisk infrastruktur som skall skyddas bedöms som tillräckliga, bör de berörda parterna koncentrera sina insatser på hot som de är sårbara för.

2.3. Principer

Följande huvudprinciper kommer att vara till ledning för genomförandet av EPCIP:

- **Subsidiaritet** – Kommissionens insatser kommer att inriktas på kritisk infrastruktur ur ett europeiskt snarare än ett nationellt eller regionalt perspektiv. Trots detta kan kommissionen på begäran bistå medlemsstater i fråga om nationell kritisk infrastruktur, med förbehåll för att gemenskapen är behörig och har tillgängliga resurser.

- **Komplementaritet** – Kommissionen kommer att undvika överlappningar med insatser som redan görs på EU-nivå eller nationellt eller regionalt, när dessa har visat sig effektiva för att skydda kritisk infrastruktur. EPCIP kommer således att komplettera och bygga vidare på befintliga åtgärder på sektorsnivå.

- **Sekretess** – Information om kritisk infrastruktur (CIPI) kommer att sekretessbeläggas på lämpligt sätt både på EU-nivå och i medlemsstaterna. Tillgången till systemet kommer att vara förbehållen personer som verkligen är i behov av uppgifterna. Utbytet av information om kritiskt infrastruktur kommer att ske i en atmosfär att tillit och säkerhet.

- **Samarbete mellan berörda aktörer** – Alla berörda aktörer kommer, så långt det är möjligt, att involveras i utvecklingen och genomförandet av EPCIP. Det kommer att omfatta ägare/operatörer av sådan kritisk infrastruktur som klassificeras som europeisk kritisk infrastruktur samt offentliga myndigheter och andra relevanta organ.

- **Proportionalitet** – Åtgärder kommer endast att föreslås när ett behov kan konstateras efter en analys av befintliga säkerhetsbrister. Åtgärderna skall vara proportionella i förhållande till risknivån och typen av hot.

- **Sektorsbaserad strategi** – Eftersom olika sektorer har sina särskilda erfarenheter, sakkunskaper och krav när det gäller skyddet av kritisk infrastruktur, kommer EPCIP att utvecklas på sektorsbasis och genomföras i enlighet med en förteckning över sektorer med kritisk infrastruktur, som berörda aktörer har enats om.

2.4. En ram för EPCIP

Ramen kommer att bestå av följande:

- Ett förfarande för fastställande och klassificering av europeisk kritisk infrastruktur (ECI), och en gemensam strategi för bedömning av behoven av ett förbättrat skydd av sådan infrastruktur. Ett sådant förfarande kommer att införas genom ett direktiv.

- Åtgärder för att underlätta genomförandet av EPCIP, inklusive en handlingsplan för EPCIP, nätverket för varningar om hot mot kritisk infrastruktur (CIWIN),

användningen av grupper av experter på skydd av kritisk infrastruktur på EU-nivå, förfaranden för utbyte av information om skydd av kritisk infrastruktur samt identifiering och analys av ömsesidiga beroendeförhållanden.

- Stöd till medlemsstater i fråga om kritisk infrastruktur vilket enskilda medlemsstater kan välja att använda sig av. I detta meddelande fastställs en grundläggande strategi för skydd av nationell kritisk infrastruktur.

- Beredskapsplaner.

- En yttre dimension.

- Kompletterande finansiella åtgärder, särskilt EU-programmet ”Terrorism – förebyggande, beredskap och konsekvenshantering och andra säkerhetsrelaterade risker” för perioden 2007–2013”, som kommer att ge möjlighet till finansiering av åtgärder rörande skydd av kritisk infrastruktur som kan överföras inom EU.

Var och en av dessa åtgärder tas upp nedan.

2.5. Kontaktgruppen för skydd av kritisk infrastruktur

Det behövs en mekanism på EU-nivå som kan tjäna som grund för den strategiska samordningen och det strategiska samarbetet och driva arbetet med de allmänna aspekterna av EPCIP och sektorsspecifika åtgärder framåt. Därför kommer en kontaktgrupp för skydd av kritisk infrastruktur att inrättas.

Kontaktgruppen kommer att bestå av kontaktpunkterna för skydd av kritisk infrastruktur från varje medlemsstat och ledas av kommissionen. Varje medlemsstat bör utse en kontaktpunkt för skydd av kritisk infrastruktur som samordnar frågor om skydd av kritisk infrastruktur inom den egna medlemsstaten och med andra medlemsstater, rådet och kommissionen. Att man utser en kontaktpunkt för skydd av kritisk infrastruktur hindrar inte att andra myndigheter i en medlemsstat deltar i behandlingen av frågor om skydd av kritisk infrastruktur.

3. EUROPEISK KRITISK INFRASTRUKTUR (ECI)

Europeisk kritisk infrastruktur är den kritiska infrastruktur som bedömts vara av största betydelse för gemenskapen och som, om den skadades eller förstördes, skulle påverka två eller fler medlemsstater, eller en enskild medlemsstat om den kritiska infrastrukturen är belägen i en annan medlemsstat. Detta inkluderar gränsöverskridande verkningar till följd av ömsesidiga beroendeförhållanden mellan sammanlänkad infrastruktur som hör till olika sektorer. Förfarandet för att fastställa och klassificera europeisk kritisk infrastruktur och en gemensam strategi för bedömning av behoven av ett förbättrat skydd av sådan infrastruktur kommer att regleras i ett direktiv.

4. ÅTGÄRDER FÖR ATT UNDERLÄTTA UTVECKLINGEN OCH GENOMFÖRANDET AV EPCIP

Kommissionen kommer att använda sig av ett antal åtgärder för att underlätta genomförandet av EPCIP och främja arbetet med skydd av kritisk infrastruktur på EU-nivå.

4.1. Handlingsplanen för EPCIP

EPCIP kommer att vara en fortlöpande process som ses över regelbundet inom ramen för handlingsplanen för EPCIP. I handlingsplanen anges vilka insatser som skall genomföras och vilka tidsfrister som gäller för dessa insatser. Handlingsplanen (som återfinns i bilagan) kommer att uppdateras regelbundet med hänsyn till hur arbetet utvecklar sig.

I handlingsplanen för EPCIP koncentreras verksamheten rörande skydd av kritisk infrastruktur till tre områden:

- Område 1: De strategiska aspekterna av EPCIP och utvecklingen av åtgärder som kan tillämpas övergripande på allt arbete som rör skydd av kritisk infrastruktur.

- Område 2: Rör europeisk kritisk infrastruktur och genomförs på sektorsnivå.

- Område 3: Stöd till medlemsstaterna i deras verksamheter rörande nationell kritisk infrastruktur.

Vid genomförandet av handlingsplanen för EPCIP kommer hänsyn att tas till specifika förhållanden inom de enskilda sektorerna. I lämpliga fall kommer även andra berörda aktörer att involveras.

4.2. Nätverket för varningar om hot mot kritisk infrastruktur (CIWIN)

Nätverket för varningar om hot mot kritisk infrastruktur (CIWIN) kommer att inrättas genom ett separat kommissionsförslag, varvid vederbörlig hänsyn kommer att tas till behovet att undvika överlappningar. Nätverket kommer att fungera som bas för utbyte av god praxis under säkra förhållanden. CIWIN är ett komplement till befintliga närverk och skulle även kunna utgöra en alternativ plattform för utbyte av snabba varningar, kopplad till kommissionens Argus-system. Den nödvändiga säkerhetsprövningen för att garantera att säkerhetskraven är uppfyllda kommer att ske i enlighet med relevanta förfaranden.

4.3. Expertgrupper

En dialog mellan de berörda aktörerna är av avgörande betydelse om man skall kunna förbättra skyddet av kritisk infrastruktur i EU. I de fall det behövs särskild sakkunskap kan kommissionen inrätta expertgrupper på EU-nivå för skydd av kritisk infrastruktur. Dessa skulle ta sig an tydligt definierade frågeställningar och underlätta dialogen mellan den offentliga och den privata sektorn i frågor som rör skydd av kritisk infrastruktur. Expertgrupperna skall stödja EPCIP genom att underlätta utbytet av synpunkter i frågor som rör skydd av kritisk infrastruktur och fylla en rådgivande funktion. Det rör sig om en frivillig mekanism där offentliga och privata resurser blandas för att uppnå ett mål eller en uppsättning mål som bedöms vara till ömsesidig nytta såväl för medborgarna som för den privata sektorn.

Expertgrupperna kommer inte att ersätta andra grupper som redan har inrättats eller som skulle kunna anpassas så att de uppfyller behoven i samband med EPCIP. De kommer inte heller att vara involverade i direkt utbyte av uppgifter mellan näringslivet, medlemsstaternas myndigheter och kommissionen.

På EU-nivå kommer expertgrupperna att ha ett klart formulerat mål och en tidsram inom vilken målet skall uppnås. Det skall också vara klart definierat vilka som kan bli medlemmar. Expertgrupperna skall upplösas när de fastställda målen är uppnådda.

Expertgruppernas funktioner kan variera mellan olika sektorer för skydd av infrastruktur, med hänsyn till vad som är karakteristiskt för den enskilda sektorn. Dessa funktioner kan omfatta följande uppgifter:

- Bistå med att definiera sårbarhet, ömsesidigt beroende och bästa praxis inom en sektor.
- Bistå vid utarbetandet av åtgärder för att minska och/eller undanröja allvarlig sårbarhet och vid utvecklingen av resultatindikatorer.
- Underlätta informationsutbyte, fortbildning och uppbyggnad av ömsesidigt förtroende på området.
- Utveckla och framhålla ”konkreta typfall” för att till andra verksamheter inom sektorn förmedla värdet av att medverka i planer och initiativ när det gäller skydd av infrastruktur.
- Tillhandahålla sektorsspecifika sakkunskaper och råd om olika ämnen, till exempel forskning och utveckling.

4.4. Informationsutbytet när det gäller skydd av kritisk infrastruktur

Utbytet av information om skydd av kritisk infrastruktur mellan de relevanta berörda aktörerna förutsätter ett ömsesidigt förtroende, så att de förtroliga, känsliga eller personliga uppgifter, som har utbytts frivilligt, inte offentliggörs, och att känsliga uppgifter omfattas av tillräckligt skydd. I detta sammanhang är det viktigt att ta hänsyn till behovet av skydd för privatlivet.

Berörda aktörer skall vidta lämpliga åtgärder för att skydda uppgifter om till exempel säkerheten vid kritisk infrastruktur och skyddade system, undersökningar om ömsesidiga beroendeförhållanden samt sårbarhets-, hot- och riskbedömningar i anslutning till skydd av kritisk infrastruktur. Sådan information kommer bara att användas till att skydda kritisk infrastruktur. Alla personer som hanterar konfidentiella uppgifter skall ha genomgått en säkerhetsprövning av den medlemsstat där personen i fråga är medborgare.

Vid utbytet av uppgifter rörande skydd av kritisk infrastruktur är det dessutom viktigt att ta hänsyn till att vissa uppgifter, även om de inte är klassade som konfidentiella, ändå kan vara av känslig natur och därför bör behandlas försiktigt.

Utbytet av uppgifter om skydd av kritisk infrastruktur kommer att ge följande verkningar:

- Förbättrad och mer precis information och förståelse av ömsesidigt beroende, hot, sårbarhet, säkerhetsincidenter, motåtgärder och bästa praxis när det gäller skydd av kritisk infrastruktur.
- Ökad medvetenhet om frågor rörande kritisk infrastruktur.
- Dialog mellan berörda aktörer.
- Mer välfokuserade insatser när det gäller fortbildning och forskning och utveckling.

4.5. Identifiering av ömsesidigt beroende

Kartläggningen och analysen av det ömsesidiga beroendet, som är både geografiskt och sektorsanknutet till sin natur, kommer att vara en viktig faktor när det gäller att förbättra skyddet av kritisk infrastruktur i EU. Resultaten av denna fortlöpande process kommer att inverka på bedömningen av sårbarhet, hot och risker i samband med kritisk infrastruktur i EU.

5. NATIONELL KRITISK INFRASTRUKTUR

Med vederbörlig hänsyn till gemenskapens befintliga befogenheter ligger ansvaret för nationell kritisk infrastruktur på ägarna och operatörerna av infrastrukturen och på medlemsstaterna. Kommissionen kommer att stödja medlemsstaterna i detta arbete när medlemsstaterna så begär.

Med hänsyn till strävan att förbättra skyddet av nationell kritisk infrastruktur, uppmanas varje medlemsstat att inrätta ett nationellt program för skydd av kritisk infrastruktur. Syftet med dessa program skulle vara att fastställa varje medlemsstats strategi för skyddet av nationell kritisk infrastruktur som är belägen inom dess territorium. Sådana program skulle åtminstone omfatta följande frågor:

- Den berörda medlemsstatens kartläggning och klassificering av nationell kritisk infrastruktur i enlighet med på förhand fastställda nationella kriterier. Dessa kriterier skulle fastställas av den enskilda medlemsstaten, med hänsyn till åtminstone följande kvalitativa och kvantitativa verkningar av att en viss infrastruktur drabbas av driftsstörningar eller förstörs:

    - Omfattning – Driftsstörningen vid eller förstörelsen av en viss kritisk infrastruktur kommer att bedömas utifrån omfattningen på det geografiska område som skulle kunna påverkas av att infrastrukturen går förlorad eller upphör att fungera.

    - Verkningar – Verkningarna av att en viss infrastruktur drabbas av driftsstörningar eller förstörs kommer att bedömas på grundval av följande kriterier:

    – Verkningar för befolkningen (antal människor i befolkningen som påverkas).

    – Ekonomiska verkningar (omfattningen av ekonomiska förluster och/eller försämring av varor och tjänster).

    – Miljöpåverkan.

    – Politiska konsekvenser.

    – Psykologiska verkningar.

    – Konsekvenser för folkhälsan

    Om sådana kriterier inte finns kommer kommissionen att hjälpa medlemsstater som begär det att utveckla sådana kriterier genom att förmedla relevanta metoder.

- Införande av en dialog mellan ägare och operatörer av kritisk infrastruktur.

- Kartläggning av ömsesidigt beroende geografiskt och sektorsvis.

- Inrättande av beredskapsplaner för nationell kritisk infrastruktur när det bedöms som relevant.

- Varje medlemsstat uppmuntras att basera sitt nationella program för skydd av kritisk infrastruktur på den gemensamma förteckning över sektorer med kritisk infrastruktur som fastställts med avseende på europeisk kritisk infrastruktur.

Om liknande strategier infördes för skyddet av nationell kritisk infrastruktur i medlemsstaterna skulle detta bidra till att berörda aktörer på infrastrukturområdet i hela EU kunde slippa nackdelen att behöva ta hänsyn till olika regelverk, vilket skulle minska deras kostnader och risken för snedvridning av konkurrensen på den inre marknaden.

6. BEREDSKAPSPLANER

Beredskapsplaner är ett nyckelinslag i processen att skydda kritisk infrastruktur, eftersom de gör det möjligt att minimera de potentiella verkningarna av att kritisk infrastruktur drabbas av driftsstörningar eller förstörs. Utvecklingen av en övergripande strategi för utarbetandet av beredskapsplaner, som omfattar sådana frågor som medverkan från ägare och operatörer av kritisk infrastruktur, samarbete med nationella myndigheter och utbyte av information mellan grannländer bör vara ett viktigt inslag i genomförandet av EPCIP.

7. DEN YTTRE DIMENSIONEN

Terrorism och annan brottslighet samt naturkatastrofer och andra olycksorsaker känner inga nationsgränser. Hoten kan med andra ord inte ses enbart ur ett nationellt perspektiv. Följaktligen måste full hänsyn tas till den yttre dimensionen vid genomförandet av EPCIP. Vår tids ekonomier och samhällen är så sammanlänkade och ömsesidigt beroende av varandra att även en driftsstörning utanför EU:s gränser kan få allvarliga konsekvenser för gemenskapen och dess medlemsstater. På samma sätt kan EU:s partner drabbas av skadliga verkningar om kritisk infrastruktur inom EU drabbas av driftsstörningar eller förstörs. Genom att arbeta för målet att öka skyddet för kritisk infrastruktur i EU, kan man minska risken för störningar av EU:s ekonomi och därigenom bidra till EU:s konkurrenskraft på det globala planet.

En utvidgning av insatserna för ökat samarbete till områden utanför EU, till exempel genom sektorsspecifika samförståndsavtal (om exempelvis utvecklingen av gemensamma standarder, genomförandet av gemensamma undersökningar rörande skydd av kritisk infrastruktur, fastställande av gemensamma typer av hot och utbyte av bästa praxis om skyddsåtgärder), och insatser för att uppmuntra högre standarder när det gäller skydd av kritisk infrastruktur utanför EU bör därför ingå som en viktig del av EPCIP. Ett yttre samarbete om skydd av kritisk infrastruktur kommer i huvudsak att vara inriktat på EU:s grannar. Med hänsyn till den globala sammankopplingen av vissa sektorer, till exempel informationstekniksektorn och finansmarknaderna, skulle en mer global strategi också vara berättigad. Dialog och utbyte av bästa praxis bör således involvera alla relevanta EU-partner och internationella organisationer. Kommissionen kommer också att fortsätta att främja förbättringar av skyddet av kritisk infrastruktur i länder utanför EU genom att inom ramen för redan existerande strukturer och politik, inklusive ”stabilitetsinstrumentet”, arbeta tillsammans med partner inom G8, Euromed och den europeiska grannskapspolitiken

8. ÅTFÖLJANDE FINANSIELLA ÅTGÄRDER

Gemenskapsprogrammet ”Terrorism – förebyggande, beredskap och konsekvenshantering och andra säkerhetsrelaterade risker” för perioden 2007–2013” kommer att bidra till genomförandet av EPCIP.

Förutsatt att programmet inte finansieras på annat sätt kommer det att inom sina allmänna ramar stimulera, främja och utveckla åtgärder för förebyggande åtgärder, beredskap och konsekvenshantering som syftar till att förebygga eller reducera alla säkerhetsrisker, särskilt risker med koppling till terrorism, i lämpliga fall grundat på omfattande hot- och riskbedömningar.

Finansiering inom programmet, genom bidrag och åtgärder som initierats av kommissionen, kommer särskilt att användas till utveckling av instrument, strategier, metoder, studier, bedömningar, åtgärder och insats er på området effektivt skydd av kritisk infrastruktur (både på EU-nivå och i medlemsstaterna).

BILAGA

Handlingsplan för europeiska programmet för skydd av kritisk infrastruktur

Område 1: Konsekutiva strategier för skydd av kritisk infrastruktur

Område 1 kommer att fungera som strategisk plattform för den övergripande samordningen av europeiska programmet för skydd av kritisk infrastruktur och samarbetet genom EU:s kontaktgrupp för skydd av kritisk infrastruktur.

Etapp 1

Åtgärd	Aktör	Tidsram
Utveckling av gemensamma sektorsbaserade definitioner och terminologi för arbetet med kritisk infrastruktur	Kommissionen, medlemsstaterna och ibland andra berörda aktörer	Senast ett år efter det att direktivet om ett europeiskt program för skydd av kritisk infrastruktur trätt i kraft
Utarbetande av allmänna kriterier som skall användas för att kartlägga europeisk kritisk infrastruktur	Kommissionen, medlemsstaterna och ibland andra berörda aktörer	Senast ett år efter det att direktivet om ett europeiskt program för skydd av kritisk infrastruktur trätt i kraft
Inrättande av ett inventarium över nationella, bilaterala och EU-övergripande program för kritisk infrastruktur	Kommissionen och medlemsstaterna	Pågående
Skapande av och överenskommelse om riktlinjer om insamling och användning av känsliga uppgifter mellan berörda parter	Kommissionen, medlemsstaterna och ibland andra berörda parter	Pågående
Insamling av bästa praxis för skydd av kritisk infrastruktur, riskbedömning och metoder	Kommissionen, medlemsstaterna och ibland andra berörda parter	Pågående
Genomförande av studier om ömsesidiga beroendeförhållanden	Kommissionen, medlemsstaterna och ibland andra berörda parter	Pågående

Etapp 2

Åtgärd	Aktör	Tidsram
Kartläggning av brister där gemenskapsinitiativ skulle innebära ett	Kommissionen, medlemsstaterna och	Pågående

mervärde	ibland andra berörda parter	
Inrättande av sektorsvisa EU-grupper med sakkunnig inom skydd av kritisk infrastruktur	Kommissionen, medlemsstaterna och ibland andra berörda parter	Pågående
Kartläggning av förslag till åtgärder för att skydda kritisk infrastruktur som kan finansieras på EU-nivå	Kommissionen och medlemsstaterna	Pågående
Införande av EU-finansiering av åtgärder för att skydda kritisk infrastruktur	Kommissionen	Pågående

Etapp 3

Åtgärd	Aktör	Tidsram
Inledande av samarbete med tredjeländer och internationella organisationer	Kommissionen och medlemsstaterna	Pågående

Insatsväg 2: Skydd av europeisk kritisk infrastruktur

Inom ramen för insatsväg 2 kommer minskad sårbarhet för europeisk kritisk infrastruktur att betonas

Etapp 1

Åtgärd	Aktör	Tidsram
Utarbetande av sektorsspecifika kriterier som skall användas för att kartlägga europeisk kritisk infrastruktur	Kommissionen, medlemsstaterna och ibland andra berörda parter	Senast ett år efter det att direktivet om ett europeiskt program för skydd av kritisk infrastruktur trätt i kraft

Etapp 2

Åtgärd	Aktör	Tidsram
Kartläggning och verifiering sektor för sektor av kritisk infrastruktur som sannolikt kommer att klassificeras som kritisk infrastruktur	Kommissionen och medlemsstaterna	Senast ett år efter antagandet av relevanta kriterier och därefter fortlöpande
Utnämnandet av europeisk kritisk infrastruktur	Kommissionen och medlemsstaterna	Pågående
Kartläggning av sårbarhet, hot och risker mot särskild europeisk kritisk infrastruktur	Kommissionen, medlemsstaterna, ägare till och	Senast ett år efter att infrastrukturens definierats som

inklusive utarbetandet av säkerhetsplaner	operatörer av europeisk kritisk infrastruktur (allmän rapport till kommissionen)	europeisk kritisk infrastruktur
Bedömning av behovet av skyddsåtgärder och åtgärder på EU-nivå	Kommissionen, medlemsstater och ibland andra berörda parter	Senast ett och ett halvt år efter utnämnandet av europeisk kritisk infrastruktur
Bedömning av de enskilda medlemsstaternas strategier för varningsnivåer för infrastruktur som definieras som europeisk kritisk infrastruktur. Inledning av en genomförbarhetsstudie om kalibrering eller harmonisering av sådana varningar.	Kommissionen och medlemsstaterna	Pågående

Etapp 3

Åtgärd	Aktör	Tidsram
Utveckling och antagande av förslag till lägsta skyddsåtgärder avseende europeisk kritisk infrastruktur	Kommissionen, medlemsstaterna, ägare och operatörer av europeisk kritisk infrastruktur	Efter bedömning av huruvida det krävs skyddsåtgärder och åtgärder på EU-nivå
Genomförande av lägsta skyddsåtgärder	Medlemsstaterna samt ägare och operatörer av europeisk kritisk infrastruktur	Pågående

Insatsväg 3: Stöd avseende nationell kritisk infrastruktur

Insatsväg 3 är en mellanstatlig insatsväg för att hjälpa medlemsstaterna i sitt skydd av nationell kritisk infrastruktur

Etapp 1

Åtgärd	Aktör	Tidsramar
Informationsutbyte om de kriterier som tillämpas för att kartlägga nationell kritisk infrastruktur	Medlemsstaterna (på begäran kan kommissionen bistå medlemsstaten)	Pågående

Etapp 2

Åtgärd	Aktör	Tidsram
Kartläggning och verifiering av sektorsspecifik kritisk infrastruktur som sannolikt kommer att klassificeras som nationell kritisk infrastruktur	Medlemsstaterna och ibland andra berörda parter	Pågående
Utnämning av specifik kritisk infrastruktur som nationell kritisk infrastruktur	Medlemsstaterna	Pågående
Analys sektor för sektor av existerande säkerhetsluckor i den nationella kritiska infrastrukturen.	Medlemsstaterna och ibland andra berörda parter (på begäran kan kommissionen bistå medlemsstaten)	Pågående

Etapp 3

Åtgärd	Aktör	Tidsram
Inrättande och utveckling av nationella program för skydd av kritisk infrastruktur	Medlemsstaterna (på begäran kan kommissionen bistå medlemsstaten)	Pågående
Utveckling av specifika skyddsåtgärder för varje nationell kritisk infrastruktur	Medlemsstaterna, nationell kritisk infrastruktur (på begäran kan kommissionen bistå medlemsstaten)	Pågående
Övervakning av att ägare eller operatörer vidtar nödvändiga genomförandeåtgärder	Medlemsstaterna	Pågående