EIROPAS KOPIENU KOMISIJA

Briselē, 17.11.2005
COM(2005) 576 galīgā redakcija

ZAĻĀ GRĀMATA

PAR EIROPAS PROGRAMMU KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAI

(iesniegusi Komisija)

ZAĻĀ GRĀMATA

PAR EIROPAS PROGRAMMU KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAI

1. VISPĀRĪGA INFORMĀCIJA

Tīši terorisma akti, stihiskas nelaimes, nolaidība, nelaimes gadījumi vai nesankcionēta ielaušanās datorsistēmās, noziedzīga darbība un ļaunprātīga rīcība var bojāt un iznīcināt kritisko infrastruktūru (KI) vai izraisīt tās funkciju pārtraukšanu. Lai glābtu to cilvēku dzīvību un īpašumu ES, ko apdraud terorisms, stihiskas nelaimes un nelaimes gadījumi, jebkāda veida KI funkciju pārtraukšanai vai ar KI veiktajām manipulācijām ir jābūt, cik iespējams, īslaicīgām, retām, pārvaldāmām, ģeogrāfiski norobežotām un tādām, kuru radītais kaitējums dalībvalstīm, to iedzīvotājiem un Eiropas Savienībai ir minimāls. Nesenie teroristu uzbrukumi Madridē un Londonā vērsa uzmanību uz teroristu uzbrukumu draudiem Eiropas infrastruktūrām. ES atbildes pasākumiem ir jābūt nekavējošiem, saskaņotiem un efektīviem.

Eiropadome 2004. gada jūnija sanāksmē pieprasīja Komisijai sagatavot vispārēju stratēģiju kritiskās infrastruktūras aizsardzībai. Tāpēc 2004. gada 20. oktobrī Komisija pieņēma paziņojumu „Kritisko infrastruktūru aizsardzība cīņā pret terorismu", sniedzot konkrētus ierosinājumus par to, kas veicinātu teroristu uzbrukumu novēršanu, gatavību un reaģēšanu uz tiem saistībā ar kritiskajām infrastruktūrām.

Padome 2004. gada decembrī pieņemtajos secinājumos par „Teroristu uzbrukumu novēršanu, gatavību un reaģēšanu uz tiem" un „ES Solidaritātes programmu par teroristu draudu un uzbrukumu sekām" apstiprināja Komisijas iniciatīvu ierosināt Eiropas programmu kritisko infrastruktūru aizsardzībai (EPKIA) un piekrita kritiskās infrastruktūras brīdinājuma informācijas tīkla (KIBIT) izveidei, ko veic Komisija.

Komisija organizēja divus seminārus un aicināja dalībvalstis sniegt idejas un komentārus. Pirmais seminārs ar dalībvalstu piedalīšanos par ES kritiskās infrastruktūras aizsardzību notika no 2005. gada 6. jūnija līdz 7. jūnijam. Pēc semināra dalībvalstis iesniedza Komisijai attiecīgus pamatinformācijas dokumentus par viņu īstenoto pieeju kritiskās infrastruktūras aizsardzībai (KIA) un sniedza komentārus par seminārā apspriestajām idejām. Iesniegumi tika saņemti jūnijā un jūlijā, un tos izmantoja par pamatu KIA turpmākai pilnveidošanai. Otrais seminārs par ES KIA notika no 12. līdz 13. septembrim, lai turpinātu diskusijas par KIA jautājumiem. Otrajā seminārā piedalījās gan dalībvalstis, gan ražošanas asociācijas. Rezultātā Komisija pieņēma lēmumu iesniegt šo zaļo grāmatu, kurā izklāstītas EPKIA paredzētie risinājumi.

2. ZAĻĀS GRĀMATAS MĒRĶIS

Zaļās grāmatas galvenais mērķis ir, iesaistot plašu ieinteresēto personu loku, saņemt atsauksmes par iespējamiem EPKIA politiskajiem risinājumiem. Lai nodrošinātu efektīvu kritiskās infrastruktūras aizsardzību, ir nepieciešama saziņa, koordinēšana un sadarbība starp visām ieinteresētajām personām (kritiskās infrastruktūras īpašniekiem un apsaimniekotājiem, reglamentējošajām institūcijām, profesionālajām struktūrām un ražošanas asociācijām) sadarbībā ar visu līmeņu valsts pārvaldi un sabiedrību.

Zaļajā grāmatā izklāstīti Komisijas risinājumi, atbildot uz Padomes pieprasījumu ieviest EPKIA un KIBIT, un tā ietilpst konsultāciju par Eiropas programmu kritisko infrastruktūru aizsardzībai otrajā posmā. Komisija sagaida, ka, iesniedzot šo zaļo grāmatu, tā saņems konkrētas atsauksmes par šajā dokumentā izklāstītajiem politiskajiem risinājumiem. Atkarībā no konsultāciju rezultāta EPKIA politiku plānu varētu iesniegt 2006. gadā.

3. EPKIA MĒRĶIS UN JOMA

3.1. EPKIA vispārējais mērķis

EPKIA mērķis būtu nodrošināt pienācīgus un vienādus kritiskās infrastruktūras aizsardzības līmeņus, līdz minimumam samazināt kļūmes un nodrošināt ātrus, pārbaudītus atjaunošanas līdzekļus visā ES. Visiem kritiskās infrastruktūras objektiem nav iespējams nodrošināt vienādu aizsardzības līmeni; to var ietekmēt KI nepilnības. EPKIA pastāvīgi mainīsies; tā regulāri tiks no jauna izvērtēta atkarībā no aktuāliem jautājumiem un problēmām.

EPKIP ir pēc iespējas jāsamazina jebkāda negatīva ietekme, ko pieaugošais ieguldījumu apjoms drošības nodrošināšanai varētu radīt konkurencei noteiktā nozarē. Aprēķinot izmaksas samērīgumu, nedrīkst atstāt bez ievērības nepieciešamību saglabāt tirgu stabilitāti, kas ir būtiska attiecībā uz ilgtermiņa ieguldījumiem, kā arī drošības radīto ietekmi uz vērtspapīru tirgu attīstību un makroekonomiku.

Jautājums

Vai šis EPKIA mērķis ir pienācīgs? Ja nē, kādam vajadzētu būt mērķim?

3.2. Pret ko EPKIA būtu jāaizsargā?

Lai arī seku pārvarēšanas pasākumi attiecībā uz lielāko daļu funkciju pārtraukšanas gadījumu ir vienādi vai līdzīgi, aizsardzības pasākumi var atšķirties atkarībā no apdraudējuma veida. Draudi, kas var būtiski samazināt iespējas nodrošināt iedzīvotāju pamatvajadzības un drošību, uzturēt kārtību un nodrošināt svarīgāko publisko pakalpojumu minimumu vai pienācīgu ekonomikas funkcionēšanu, var būt gan apzināti uzbrukumi, gan stihiskas nelaimes. Iespējamie risinājumi ir šādi:

a) **jebkāda veida apdraudējuma gadījumā izmantojama pieeja** – tā būtu visaptveroša pieeja, kas paredz gan apzinātu uzbrukumu, gan stihisku nelaimju draudus. Tā nodrošinātu, ka sinerģijas starp aizsardzības pasākumiem tiek maksimāli izmantotas, bet terorismam netiktu pievērsta pastiprināta uzmanība;

b) **jebkāda veida apdraudējuma gadījumā izmantojama pieeja, par prioritāriem uzskatot terorisma draudus** – tā būtu elastīga pieeja, kas nodrošina saikni ar citiem apdraudējuma veidiem, piemēram, apzinātu uzbrukumu draudiem, kā arī stihiskām nelaimēm, bet par prioritāriem uzskatot terorisma draudus. Ja aizsardzības pasākumu līmeni noteiktā rūpniecības nozarē atzītu par pienācīgu, ieinteresētās personas koncentrētu uzmanību uz tiem draudiem, no kuriem tās vēl nav pasargātas;

c) **terorisma draudu gadījumā izmantojama pieeja** - tā būtu pieeja, kurā galvenā uzmanība būtu veltīta terorisma draudiem nevis biežāk sastopamiem apdraudējuma veidiem.

Jautājums
Kuru pieeju vajadzētu izvēlēties EPKIA? Kāpēc?

4. IEROSINĀTIE PAMATPRINCIPI

EPKIA ir ierosināts balstīt uz šādiem pamatprincipiem.

- **Subsidiaritāte** – subsidiaritāte būtu EPKIA pamatā, nodrošinot, ka kritisko infrastruktūru aizsardzība vispirms ir valsts kompetences jautājums. Saistībā ar kritisko infrastruktūru aizsardzību galvenā atbildība būtu jāuzņemas dalībvalstij un īpašniekiem/apsaimniekotājiem, darbojoties saskaņā ar vienotu sistēmu. Savukārt Komisija galveno uzmanību pievērstu aspektiem, kas saistīti ar tādu kritisko infrastruktūru aizsardzību, kurām ES ir pārrobežu ietekme. Nevajadzētu mainīt kārtību, kas paredz īpašnieku un apsaimniekotāju atbildību un pienākumu patstāvīgi pieņemt lēmumus un izstrādāt plānus savu īpašumu aizsardzībai.

- **Komplementaritāte**– ar EPKIA vienoto sistēmu tiktu papildināti esošie pasākumi. Ja Kopienas mehānismi jau ir ieviesti, tie ir jāturpina izmantot; to izmantošana nodrošinās EPKIA vispārēju īstenošanu.

- **Konfidencialitāte** – informācijas apmaiņa attiecībā uz kritisko infrastruktūru aizsardzību tiktu īstenota, balstoties uz uzticēšanos un konfidencialitāti. Uzticēšanās un konfidencialitāte ir nepieciešama, ņemot vērā to, ka īpašas ziņas par kritisko infrastruktūru objektu var izmantot, lai izraisītu nespēju funkcionēt vai nepieņemamas sekas attiecībā uz kritiskās infrastruktūras iekārtām. Gan ES, gan dalībvalstu līmenī KIA informācija tiktu klasificēta, un pieeju tai piešķirtu tikai tad, ja ir vajadzība pēc šādas informācijas.

- **Ieinteresēto personu sadarbība** – visas ieinteresētās personas, tostarp dalībvalstis, Komisija, nozares/uzņēmējdarbības asociācijas, standartizācijas iestādes, kā arī īpašnieki, apsaimniekotāji un lietotāji („lietotāji" – organizācijas, kas ekspluatē un izmanto infrastruktūru uzņēmējdarbības un pakalpojumu sniegšanas nolūkā), piedalās KI aizsardzībā. Visām ieinteresētajām personām atbilstoši saviem uzdevumiem un atbildībai ir jāsadarbojas un jāveicina EPKIA pilnveidošana un īstenošana. Dalībvalstu iestādes saskaņā ar savu kompetenci nodrošinātu vadību un saskaņošanu tādas valsts līmeņa konsekventas pieejas izstrādē un īstenošanā, kas paredzēta kritisko infrastruktūru aizsardzībai. Īpašnieki, apsaimniekotāji un lietotāji darbotos gan vietējā, gan ES līmenī. Ja attiecīgajā nozarē nav standartu vai starptautiskas normas nav vēl ieviestas, vajadzības gadījumā standartizācijas iestādes varētu pieņemt kopējus standartus.

- **Proporcionalitāte** – aizsardzības stratēģijas un pasākumi būtu proporcionāli attiecīgā riska līmenim, jo visas infrastruktūras nav iespējams aizsargāt no visa veida draudiem (piemēram, elektropārvades tīkli ir par lielu, lai tos iežogotu vai apsargātu). Piemērojot piemērotus riska pārvaldības paņēmienus, uzmanība tiktu veltīta jomām ar visaugstāko riska pakāpi, ņemot vērā draudus, relatīvo kritiskumu, izmaksu un ieguvumu samēru, drošības pasākumu līmeni un pieejamo risku mazinošo stratēģiju efektivitāti.

Jautājums

Vai šie pamatprincipi ir pieņemami? Vai daži no tiem ir lieki? Vai ir papildus jāapsver vēl kādi principi?

Vai piekrītat, ka aizsardzības pasākumiem ir jābūt proporcionāliem attiecīgā riska līmenim, jo visas infrastruktūras nav iespējams pasargāt no visa veida draudiem?

5. EPKIA VIENOTĀ SISTĒMA

Infrastruktūras daļas bojājums vai tās zaudējums vienā dalībvalstī var negatīvi ietekmēt vairākas citas daļas un Eiropas ekonomiku kopumā. Šādas ietekmes iespēja arvien pieaug, jo jaunas tehnoloģijas (piemēram, internets) un tirgus liberalizācija (piemēram, elektroapgādes un gāzes apgādes jomā) nozīmē, ka infrastruktūra lielā mērā veido lielāku tīklu. Šādā situācijā aizsardzības pasākumi nav spēcīgāki par vājāko posmu to ķēdē. Tas nozīmē, ka var rasties nepieciešamība pēc kopēja drošības līmeņa.

Efektīvas aizsardzības nodrošināšanai ir nepieciešama saziņa, koordinēšana un sadarbība valsts, ES (attiecīgā gadījumā), kā arī starptautiskā līmenī starp visām ieinteresētajām personām. Kritisko infrastruktūru aizsardzībai Eiropā varētu ieviest vienotu ES līmeņa sistēmu, lai nodrošinātu, ka katra dalībvalsts garantē pienācīgus un vienādus aizsardzības līmeņus attiecībā uz attiecīgās dalībvalsts kritisko infrastruktūru un ka iekšējā tirgū konkurences noteikumi netiek traucēti. Lai atbalstītu dalībvalstu veiktās darbības, Komisija, sniedzot vienotu sistēmu kritisko infrastruktūru aizsardzībai, veicinātu paraugprakses identificēšanu, apmaiņu un izplatību par jautājumiem, kas saistīti ar KIA. Ir jāapsver minētās vispārējās sistēmas darbības joma.

EPKIA vienotā sistēma ietvertu vienas jomas pasākumus, ar ko nosaka visu kritisko infrastruktūru aizsardzībā (KIA) iesaistīto ieinteresēto personu kompetenci un atbildību, kā arī veido pamatu īpašām attiecīgās nozares pieejām. Vienotā sistēma ir paredzēta esošo attiecīgās nozares pasākumu papildināšanai Kopienas līmenī un dalībvalstīs, lai nodrošinātu maksimāli iespējamo drošības līmeni attiecībā uz kritiskajām infrastruktūrām Eiropas Savienībā. Darbam vienošanās panākšanai par vienotu definīciju un KI nozaru sarakstu jābūt prioritāram.

Tā kā dažādās nozares, kas saistītas ar kritiskajām infrastruktūrām, ir ļoti atšķirīgas, būtu sarežģīti precīzi noteikt, kādi kritēriji ir izmantojami, lai tās visas identificētu un aizsargātu horizontālā sistēmā; tas jāveic attiecībā uz katru nozari atsevišķi. Tomēr par atsevišķām transversālām tēmām ir nepieciešama vienota izpratne.

Tāpēc ir ierosināts stiprināt KI ES, ieviešot vienotu EPKIA sistēmu (kopīgi mērķi, metodes, piemēram, salīdzināšanai, savstarpējai atkarībai), veicot paraugprakses apmaiņu un izmantojot atbilstības uzraudzības mehānismus. Vienotajā sistēmā cita starpā būtu ietverti šādi elementi:

- kopīgi KIA principi;
- savstarpēji saskaņoti kodeksi/standarti;
- kopīgas definīcijas, uz kuru pamata iespējams vienoties par attiecīgās nozares definīcijām (1. pielikumā sniegts indikatīvs šo definīciju saraksts);
- kopējs KI nozaru saraksts (2. pielikumā sniegts indikatīvs nozaru saraksts);
- KIA prioritārās jomas;
- attiecīgo ieinteresēto personu kompetenču apraksts;

- saskaņotie paraugkritēriji;
- metodes, kas paredzētas infrastruktūru salīdzināšanai un prioritāšu noteikšanai dažādās nozarēs.

Turklāt šāda vienota sistēma samazinātu iespējamo kropļojošo ietekmi uz iekšējo tirgu.

Varētu ieviest izvēles vai obligātu EPKIA vienoto sistēmu, vai arī abas (atkarībā no jautājuma). Abi sistēmu veidi varētu papildināt spēkā esošos nozaru un horizontālos pasākumus gan Kopienas, gan dalībvalstu līmenī; tomēr tikai tiesisks regulējums nodrošinātu spēcīgu un īstenojamu tiesisko pamatu tādu pasākumu saskaņotai un vienotai īstenošanai, kas paredzēti, lai aizsargātu Eiropas Savienības kritiskās infrastruktūras (EKI), kā arī dalībvalstu un Komisijas attiecīgo kompetenču skaidrai definēšanai. Elastīgi izvēles pasākumi bez juridiskā spēka nespētu nodrošināt skaidrību par kompetencēm.

Atkarībā no rūpīgi veiktas analīzes rezultātiem, pievēršot pienācīgu vērību ierosināto pasākumu proporcionalitātei, Komisija EPKIA priekšlikumā var izmantot vairākus instrumentus, tostarp tiesību aktus. Attiecīgā gadījumā priekšlikumiem par īpašiem pasākumiem tiks pievienoti ietekmes novērtējumi.

Jautājumi

Vai vienota sistēma varētu būt efektīva KIA stiprināšanai?

Ja nepieciešams likumīgs pamats, kādi elementi tajā būtu jāietver?

Vai piekrītat, ka kritēriji, kas paredzēti, lai noteiktu dažādu veidu EKI un pasākumus, kas uzskatāmi par nepieciešamiem, ir jānosaka katrā nozarē atsevišķi?

Vai vienota sistēma būtu lietderīga, nosakot attiecīgo ieinteresēto personu kompetences? Cik lielā mērā vienotai sistēmai ir jābūt obligātai un cik – fakultatīvai?

Kādai ir jābūt vienotās sistēmas darbības jomai? Vai piekrītat indikatīvo terminu un definīciju sarakstam I pielikumā, pamatojoties uz ko katrā attiecīgā nozarē atsevišķi var veidot definīcijas (ja nepieciešams)? Vai piekrītat indikatīvo KI nozaru sarakstam II pielikumā?

6. ES KRITISKĀS INFRASTRUKTŪRAS (EKI)

6.1. ES kritiskās infrastruktūras definējums

Definējumu, kas raksturotu ES kritiskās infrastruktūras būtību, noteiktu, pamatojoties uz tās pārrobežu ietekmi, kas nosaka, vai nelaimes gadījumam varētu būt būtiska ietekme ārpus tās dalībvalsts teritorijas, kurā objekts atrodas. Šajā sakarā ir jāņem vērā arī fakts, ka divpusēji dalībvalstu sadarbības plāni KIA jomā ir vispāratzīts un efektīvs līdzeklis attiecībā uz KI starp divu dalībvalstu robežām. Šāda sadarbība papildinātu EPKIA.

EKI varētu ietvert tos fiziskos resursus, pakalpojumus, informāciju tehnoloģijas, tīklus un infrastruktūras objektus, kas gadījumā, ja tiek iznīcināti vai to darbība tiek pārtraukta, var nopietni kaitēt iedzīvotāju veselībai, drošībai, kā arī saimnieciskajai vai sociālajai labklājībai:

(a) divās vai vairāk dalībvalstīs – **tas būtu saistīts ar noteiktām divpusējām KI (vajadzības gadījumā);**

(b) trīs vai vairāk dalībvalstīs – **tas izslēgtu visas divpusējās KI.**

Apsverot minēto iespēju attiecīgās priekšrocības, ir jāņem vērā:

– infrastruktūras objekta iekļaušana EKI kategorijā nenozīmē, ka attiecībā uz to ir obligāti veicami papildu aizsardzības pasākumi. Pastāvošie aizsardzības pasākumi, kas varētu ietvert divpusējus nolīgumus starp dalībvalstīm, var būt pilnībā atbilstoši un tādējādi palikt nemainīgi, apzīmējot infrastruktūras objektu kā EKI;

– (a) iespēja varētu nozīmēt, ka lielāks skaits infrastruktūru klasificējamas kā EKI;

– (b) iespēja varētu nozīmēt, ka infrastruktūrai, kas attiecas tikai uz divām dalībvalstīm, nav Kopienas nozīmes, arī tad, ja aizsardzības līmeni viena no minētajām dalībvalstīm uzskata par nepiemērotu un otra atsakās veikt pasākumus. Bez tam (b) iespējas rezultātā varētu rasties ārkārtīgi liels divpusēju nolīgumu skaits vai strīdi starp dalībvalstīm. Nozarei, kuras darbība bieži tiek īstenota visas Eiropas līmenī, var nākties funkcionēt, pamatojoties uz virkni dažādu nolīgumu, kas var radīt papildu izmaksas.

Turklāt ir atzīts, ka jāņem vērā arī KI, kas izveidotas vai atrodas ārpus ES, bet ir savstarpēji saistītas ar ES dalībvalsti vai var to tieši ietekmēt.

Jautājums

Vai EKI vajadzētu būt infrastruktūrai, kurai ir potenciāli nopietna pārrobežu ietekme attiecībā uz divām vai vairāk dalībvalstīm vai arī uz trīs vai vairāk dalībvalstīm? Kāpēc?

6.2. Savstarpēja atkarība

Pakāpeniski identificējot visas EKI, jo īpaši ieteicams ņemt vērā savstarpēju atkarību. Savstarpējas atkarības izpēte veicinātu tādu draudu iespējamās ietekmes novērtēšanu, kas vērsti pret īpašām KI, jo īpaši lai noteiktu, kuru dalībvalsti ietekmētu nopietns incidents, kas saistīts ar KI.

Pilnībā būtu jāizvērtē savstarpēja atkarība uzņēmumos, nozaru sektoros, ģeogrāfiskajās jurisdikcijās un dalībvalstu iestādēs, jo īpaši, ja to darbība atkarīga no informācijas un telekomunikāciju tehnoloģijām (*IST*), kā arī savstarpējā atkarība starp minētajām personām. Komisija, dalībvalstis un kritisko infrastruktūru īpašnieki/apsaimniekotāji sadarbotos, nosakot savstarpēju atkarību un piemērojot atbilstošas stratēģijas, lai pēc iespējas samazinātu risku.

Jautājums

Kā varētu ņemt vērā savstarpējo atkarību?

Vai varat sniegt piemērotas metodes savstarpējās atkarības analīzei?

Kādā līmenī būtu jānotiek savstarpējās atkarības noteikšanai – ES un/vai dalībvalstu līmenī?

6.3. Īstenošanas pasākumi EKI

Attiecībā uz EKI Komisija ierosinātu šādus īstenošanas pasākumus:

(1) Komisija kopā ar dalībvalstīm katrai nozarei atsevišķi izstrādā īpašus kritērijus, kas būtu izmantojami EKI identificēšanai;

(2) pakāpeniska EKI identificēšana un pārbaude attiecīgajā nozarē, ko veic dalībvalstis un Komisija. Lēmumu par atsevišķu KI klasificēšanu kā EKI pieņems Eiropas Savienības līmenī[1], ņemot vērā attiecīgās infrastruktūras pārrobežu raksturu;

(3) dalībvalstis un Komisija analizē esošos trūkumus drošībā saistībā ar EKI katrā nozarē atsevišķi;

(4) dalībvalstis un Komisija vienojas par prioritārajām nozarēm/infrastruktūru darbības veikšanai, ņemot vērā savstarpējo atkarību;

(5) ja nepieciešams, Komisija un dalībvalstu galvenās ieinteresētās personas katrā nozarē vienojas par priekšlikumiem aizsardzības pasākumu minimumam, kas varētu ietvert arī standartus;

(6) pēc tam, kad Padome ir pieņēmusi priekšlikumus, šie pasākumi tiek īstenoti;

(7) dalībvalstis un Komisija nodrošina regulāru uzraudzību. Pārskatīšanu (attiecībā uz pasākumiem un KI identificēšanu) veic tad un tādos gadījumos, kad tā nepieciešama.

Jautājumi

Vai pasākumu saraksts attiecībā uz EKI īstenošanu ir pieņemams?

Kā jūs ieteiktu Komisijai un dalībvalstīm kopīgi identificēt EKI - dalībvalstis pieņem lēmumus svarīgos jautājumos, bet Komisija uzrauga, vai tiek ievērotas Eiropas intereses? Vai tas būtu jāīsteno ar juridiski saistošu lēmumu?

Vai ir nepieciešams arbitrāžas mehānisms, ja kāda dalībvalsts atsakās par EKI noteikt tās jurisdikcijā esošo infrastruktūru?

Vai ir nepieciešama klasifikācijas pārbaude? Kam būtu jāuzņemas atbildība?

Vai dalībvalstij vajadzētu nodrošināt iespēju klasificēt citā dalībvalstī vai trešās valstīs esošu infrastruktūru kā tādu, kas ir kritiska attiecībā uz šo dalībvalsti? Kā būtu jārīkojas, ja dalībvalsts, trešā valsts vai nozare uzskata, ka dalībvalstī esošās infrastruktūras daļa ir kritiska attiecībā uz to?

Ka būtu jārīkojas, ja attiecīgā dalībvalsts to neidentificētu? Vai ir nepieciešama pārsūdzēšanas kārtība? Ja jā, tad kāpēc?

Vai apsaimniekotājam ir jānodrošina apelācijas iespējas, ja viņš nepiekrīt veiktajai klasifikācijai vai klasifikācijas trūkumam? Ja jā, tad kāpēc?

[1] Izņemot infrastruktūras, kas saistītas ar aizsardzību.

Kādas metodes vajadzētu izstrādāt, lai noteiktu prioritārās nozares/infrastruktūras darbības veikšanai? Vai pastāv piemērotas metodes, ko var pielāgot Eiropas līmenim?

Kāda varētu būt Komisijas līdzdalība, analizējot trūkumus drošībā saistībā ar EKI?

7. VALSTU KRITISKĀS INFRASTRUKTŪRAS (VKI)

7.1. VKI nozīme attiecībā uz EPKIA

Daudzas Eiropas uzņēmējsabiedrības darbojas ārpus attiecīgās dalībvalsts robežām, un tādējādi VKI noteikumi, kas uz tām attiecas, ir atšķirīgi. Tāpēc dalībvalstu un visas ES interesēs katrai dalībvalstij ir ieteicams aizsargāt savas VKI saskaņā ar vienotu sistēmu, lai īpašniekiem un apsaimniekotājiem visā Eiropā nenāktos ciest dažādu sistēmu kopuma ievērošanas, kā rezultātā rodas pārmērīgs metožu daudzums un papildu izmaksas. Tādēļ atbilstoši Komisijas ierosinājumam EPKIA valsts kritisko infrastruktūru nevar pilnībā atstāt bez ievērības, kaut arī galvenā uzmanība ir jāvelta ES kritiskajai infrastruktūrai. Varētu paredzēt trīs risinājumus:

(a) VKI tiek pilnībā integrēta EPKIA;

(b) VKI neietilpst EPKIA darbības jomā;

(c) dalībvalstis var pēc savas iniciatīvas daļēji izmantot EPKIA attiecībā uz VKI, bet tām nav pienākuma to darīt.

Jautājums

Šķiet, ka kritiskās infrastruktūras efektīvai aizsardzībai Eiropas Savienībā būtu nepieciešama gan EKI, gan VKI identificēšana. Vai piekrītat, ka, neraugoties uz to, ka galvenā uzmanība EPKIA būtu jāvelta EKI, VKI arī nevar atstāt bez ievērības?

Kurš risinājums pēc jūsu domām ir piemērotākais EPKIA?

7.2. Valsts KIA programmas

Pamatojoties uz EPCIP vienoto sistēmu, dalībvalsts savām VKI varētu izstrādāt valsts KIA programmas. Dalībvalsts varētu piemērot pasākumus, kas ir stingrāki par EPKIA paredzētajiem.

Jautājums

Vai ir vēlams, ka katra dalībvalsts pieņem valsts KIA programmu, pamatojoties uz EPKIA?

7.3. Viena pārraudzības iestāde

Lai nodrošinātu efektivitāti un saskaņotību, ir nepieciešams, lai katra dalībvalsts nozīmētu vienu pārraudzības iestādi, kas veic EPKIA vispārēju īstenošanu. Varētu paredzēt divus risinājumus:

(a) viena KIA pārraudzības iestāde;

(b) valsts kontaktpunkts bez pilnvarām, ļaujot dalībvalstīm pašām veikt organizēšanu.

Šāda iestāde, ievērojot savu kompetenci, varētu koordinēt, uzraudzīt un pārraudzīt EPKIA īstenošanu un veikt galvenā iestāžu kontaktpunkta funkcijas KIA jautājumos attiecībā uz Komisiju, citām dalībvalstīm un KI īpašniekiem un apsaimniekotājiem. Šī iestāde varētu izraudzīties valsts pārstāvjus ekspertu grupām, kas nodarbojas ar KIA jautājumiem, un tai varētu nodrošināt pieslēgumu kritiskās infrastruktūras brīdinājuma informācijas tīklam (KIBIT). Valsts KIA koordinācijas iestāde (VKKI) varētu saskaņot valsts KIA jautājumus neatkarīgi no tā, ka citas attiecīgās dalībvalsts iestādes vai organizācijas, iespējams, jau darbojas KIA jomā.

Pakāpenisku VKI identificēšanu varētu panākt, pieprasot īpašniekiem un apsaimniekotājiem ziņot VKKI par jebkāda veida attiecīgu uzņēmējdarbību, kas saistīta ar KIA.

VKKI varētu būt atbildīga par juridiski saistošu lēmumu pieņemšanu attiecībā uz tās jurisdikcijā esošas infrastruktūras klasifikāciju kā VKI. Šāda informācija paliktu tikai attiecīgo dalībvalstu rīcībā.

Īpašās kompetences varētu ietvert:

(a) EPKIA vispārējas īstenošanas koordināciju, uzraudzību un pārraudzību dalībvalstī;

(b) galvenā iestāžu kontaktpunkta funkciju īstenošanu KIA jautājumos ar:

  i. Komisiju,

  ii. citu dalībvalsti,

  iii. KI īpašniekiem un apsaimniekotājiem;

(c) dalību ES kritiskās infrastruktūras (EKI) klasificēšanā;

(d) juridiski saistoša lēmuma pieņemšanu par to, ka tās jurisdikcijā esoša infrastruktūra klasificējama kā valsts kritiskā infrastruktūra;

(e) tiesiskas aizsardzības iestādes funkciju attiecībā uz īpašniekiem/apsaimniekotājiem, kuri nepiekrīt, ka to infrastruktūra klasificējama kā „kritiska infrastruktūra”;

(f) līdzdalību valsts kritisko infrastruktūru aizsardzības programmas un attiecīgu nozaru KIA programmu izstrādē;

(g) savstarpējo atkarību identificēšanu starp īpašām KI nozarēm;

(h) līdzdalību ekspertu grupās, lai sniegtu ieguldījumu attiecīgās nozares KIA pieeju izveidē. Varētu pieaicināt īpašnieku un apsaimniekotāju pārstāvjus, lai dotu ieguldījumu apspriedē. Varētu rīkot regulāras sanāksmes;

(i) ar KI saistītu ārkārtas rīcības plānu izstrādes uzraudzību.

Jautājumi

Vai piekrītat, ka dalībvalstij ir vienai jāuzņemas atbildība par VKI klasificēšanu un pārvaldību saskaņā ar vienotu EPKIA sistēmu?

Vai ir vēlams katrā dalībvalstī izraudzīties KIA koordinācijas iestādi, kuras pienākums ir vispārēja koordinēšana attiecībā uz pasākumiem, kas saistīti ar KIA, vienlaikus ievērojot jau pastāvošo atbildību atsevišķās nozarēs (civilās aviācijas iestādes, Seveso direktīva utt.)?

Vai ierosinātās šādas koordinācijas iestādes kompetences ir atbilstošas? Vai ir nepieciešamas vēl kādas?

7.4. Īstenošanas pasākumi VKI

Attiecībā uz VKI Komisija ierosinātu šādus īstenošanas pasākumus:

(1) izmantojot EPKIA, dalībvalstis izstrādā īpašus kritērijus, kas būtu izmantojami VKI identificēšanai;

(2) pakāpeniska VKI identificēšana un pārbaude attiecīgajā nozarē, ko veic dalībvalstis;

(3) dalībvalstis analizē esošos trūkumus drošībā saistībā ar VKI katrā nozarē atsevišķi;

(4) dalībvalstis nosaka prioritārās nozares darbības veikšanai, ņemot vērā savstarpējo atkarību un, ja vajadzīgs, ES līmenī saskaņotās prioritātes;

(5) ja vajadzīgs, attiecībā uz katru nozari dalībvalstis vienojas par attiecīgo aizsardzības pasākumu minimumu;

(6) dalībvalstis ir atbildīgas par to, lai nodrošinātu, ka to jurisdikcijā esošie īpašnieki/apsaimniekotāji veic nepieciešamo pasākumu īstenošanu;

(7) dalībvalsts nodrošina regulāru uzraudzību. Pārskatīšanu (attiecībā uz pasākumiem un KI identificēšanu) veic tad un tādos gadījumos, kad tā nepieciešama.

Jautājums

Vai pasākumu saraksts attiecībā uz VKI īstenošanu ir pienācīgs? Vai daži pasākumi ir lieki? Vai vajadzētu iekļaut vēl kādus pasākumus?

8. KI ĪPAŠNIEKU, APSAIMNIEKOTĀJU UN LIETOTĀJU FUNKCIJA

8.1. KI īpašnieku, apsaimniekotāju un lietotāju pienākumi

Klasificējot infrastruktūru kā KI, īpašniekiem un apsaimniekotājiem rodas noteikti pienākumi. Tādu infrastruktūru īpašniekiem un apsaimniekotājiem, kas klasificētas kā VKI vai EKI, varētu paredzēt četrus pienākumus:

(1) ziņot attiecīgās dalībvalsts KIA iestādei par to, ka infrastruktūra var būt kritiska;

(2) **nozīmēt vienu vai vairākus vecākos pārstāvjus veikt sadarbības koordinatora drošības jautājumos pienākumus starp īpašnieku/apsaimniekotāju un attiecīgo dalībvalsts KIA iestādi.** Sadarbības koordinators drošības jautājumos piedalītos drošības un ārkārtas rīcības plānu izstrādē. Sadarbības koordinators drošības jautājumos būtu galvenais sadarbības koordinators attiecīgajai KIA nozares iestādei dalībvalstī un, ja vajadzīgs, arī tiesībaizsardzības iestādēm;

(3) **izveidot, īstenot un atjaunināt drošības plānu apsaimniekotājiem.** Ieteicamais drošības plāns apsaimniekotājiem ir pievienots 3. pielikumā;

(4) **piedalīties ārkārtas rīcības plāna izstrādē,** kas attiecas uz KI, kopā ar attiecīgajām dalībvalsts civilās aizsardzības un tiesībaizsardzības iestādēm, ja nepieciešams.

Apsaimniekotājiem paredzēto drošības plānu varētu iesniegt apstiprināšanai attiecīgajai dalībvalsts KIA nozares iestādei, ko vispārēji uzrauga VKKI. Savukārt VKKI un, ja vajadzīgs, arī Komisija varētu īpašniekiem un apsaimniekotājiem nodrošināt attiecīgu atgriezenisko saiti un atbalstu attiecībā uz attiecīgajiem draudiem, paraugprakses izstrādi un vajadzības gadījumā sniegt palīdzību savstarpējās atkarības un neaizsargātības noteikšanai.

Katra dalībvalsts varētu noteikt termiņu, kurā VKI un EKI īpašniekiem un apsaimniekotājiem ir jāizstrādā drošības plāns apsaimniekotājiem (attiecībā uz EKI tiktu iesaistīta arī Komisija), kā arī paredzēt administratīvo naudassodu gadījumiem, ja minētais termiņš netiek ievērots.

Ir ieteikts drošības plānā apsaimniekotājiem identificēt īpašnieka/apsaimniekotāja kritiskās infrastruktūras objektus un noteikt attiecīgos drošības risinājumus to aizsardzībai. Minētajā plānā būtu aprakstītas metodes un procedūras, kas jāievēro, lai nodrošinātu atbilstību EPKIA, valsts KIA programmām un attiecīgajām KIA programmām katrā nozarē atsevišķi. Drošības plāns apsaimniekotājiem varētu nodrošināt decentralizētas pieejas īstenošanu KIA regulējumā, kas paredz lielāku rīcības brīvību (bet arī lielāku atbildību) privātajam sektoram.

Īpašās situācijās, kas skar noteiktas infrastruktūras, piemēram, elektrotīklus un informācijas tīklus, (praktisku un finansiālu apsvērumu dēļ) īpašniekiem un apsaimniekotājiem nebūtu iespējams nodrošināt vienādu drošības līmeni visiem saviem objektiem. Šādos gadījumos īpašniekiem un apsaimniekotājiem ir ieteicams kopā ar attiecīgajām iestādēm identificēt fizisko vai informācijas tīklu kritiskos punktus (mezglus), kuriem, īstenojot drošības aizsardzības pasākumus, varētu pievērst īpašu uzmanību.

Drošības plānā apsaimniekotājiem varētu ietvert drošības pasākumus, kas iedalāmi zem šādiem diviem virsrakstiem:

- „**pastāvīgie drošības pasākumi**”, kas ietvertu neaizstājamu ieguldījumu un līdzekļus drošībai, ko īpašnieks/apsaimniekotājs nevar ieviest īsā laikā. Īpašnieks/apsaimniekotājs saglabātu pastāvīgu uzmanību attiecībā uz iespējamiem draudiem, kas netraucētu viņa ierastajām saimnieciskajām, administratīvajām un sociālajām darbībām;

- „**klasificēti drošības pasākumi**”, ko varētu īstenot atbilstoši dažādiem draudu līmeņiem. Tādējādi drošības plānā apsaimniekotājiem būtu paredzēti dažādi drošības režīmi, kas pielāgoti iespējamiem to draudu līmeņiem, kas pastāv dalībvalstī, kurā atrodas attiecīgā infrastruktūra.

Ja KI īpašnieks un apsaimniekotājs neievēro pienākumu izstrādāt drošības plānu apsaimniekotājiem, piedalīties ārkārtas rīcības plānu izstrādē un nozīmēt sadarbības koordinatoru drošības jautājumos, ir ieteicams paredzēt finansiāla soda piemērošanas iespēju.

Jautājumi

Vai kritiskās infrastruktūras īpašnieku/apsaimniekotāju iespējamie pienākumi ir pieņemami attiecībā uz kritiskās infrastruktūras drošības palielināšanu? Kādas būtu viņu iespējamās izmaksas?

Vai vajadzētu noteikt, ka īpašniekiem un apsaimniekotājiem ir pienākums ziņot par to, ka viņu infrastruktūra, iespējams, ir kritiska? Kāpēc?

Vai ierosinātie pienākumi proporcionāli atbilst izmaksām, kas ar tiem saistītas?

Kādas tiesības dalībvalstu iestādēm un Komisijai vajadzētu piešķirt KI īpašniekiem un apsaimniekotājiem?

8.2. Pārrunas ar KI īpašniekiem, apsaimniekotājiem un lietotājiem

Ar EPKIA starp īpašniekiem un apsaimniekotājiem varētu nodibināt partnerattiecības. Jebkuras aizsardzības programmas panākumi ir atkarīgi no sadarbības un iesaistīšanās līmeņa, ko iespējams panākt attiecībā uz īpašniekiem un apsaimniekotājiem. Dalībvalstīs KI īpašniekus un apsaimniekotājus varētu vairāk iesaistīt KIA pilnveidē, regulāri sazinoties ar VKKI.

ES līmenī varētu organizēt forumus, lai veicinātu viedokļu apmaiņu par vispārīgiem un attiecīgu nozaru KIA jautājumiem. Attiecībā uz privātā sektora iesaistīšanos ar KIA saistītu jautājumu risināšanā vienota pieeja, kas paredz visu valsts un privāto jomu ieinteresēto personu ciešāku sadarbību, nodrošinātu dalībvalstīm, Komisijai un nozarei svarīgu platformu jebkuru radušos KIA jautājumu apspriešanai. KI īpašnieki, apsaimniekotāji un lietotāji varētu palīdzēt izstrādāt vienotas pamatnostādnes, paraugprakses standartus un, ja vajadzīgs, veikt attiecīgās informācijas apmaiņu. Šādas pārrunas palīdzētu sagatavot turpmāko EPKIA pārskatīšanu.

Ja vajadzīgs, Komisija varētu rosināt ar ES KIA saistītu nozaru/profesionālo apvienību izveidi. Divi svarīgākie mērķi būtu nodrošināt Eiropas ražotāju konkurētspējas saglabāšanu un ES iedzīvotāju drošības uzlabošanu.

Jautājums

Kādai vajadzētu būt KI īpašnieku, apsaimniekotāju un lietotāju pārrunu struktūrai?

Kam vajadzētu pārstāvēt īpašniekus, apsaimniekotājus un lietotājus pārrunās starp valsts un privāto sektoru?

9. EPKIA ATBALSTA PASĀKUMI

9.1. Kritiskās infrastruktūras brīdinājuma informācijas tīkls (KIBIT)

Komisija ir izstrādājusi vairākas ātrās reaģēšanas sistēmas, kas nodrošina precīzu, saskaņotu un efektīvu reaģēšanu ārkārtas situācijās, tostarp tādās, kas saistītas ar terorismu. Komisija 2004. gada 20. oktobrī paziņoja par tāda centrālā tīkla izveidi Komisijā, kas nodrošina ātru informācijas plūsmu starp visām Komisijas ātrās reaģēšanas sistēmām un attiecīgajiem Komisijas dienestiem (*ARGUS*).

Komisija ierosina izveidot KIBIT, kas varētu veicināt pienācīgu aizsardzības pasākumu pilnveidi, atvieglinot paraugprakses apmaiņu drošā veidā, kā arī sniegt informāciju par tūlītējiem draudiem un trauksmēm. Sistēma nodrošinātu, ka attiecīgo cilvēku rīcībā attiecīgā laikā ir attiecīgā informācija.

KIBIT izstrādei ir iespējami šādi trīs risinājumi:

(1) **KIBIT varētu būt foruma veidā, nodrošinot tikai ideju un paraugprakses par KIA apmaiņu,** lai atbalstītu KI īpašniekus un apsaimniekotājus. Šādu forumu varētu organizēt ekspertu tīkla veidā, kā arī ar elektroniskas platformas starpniecību attiecīgās informācijas apmaiņai drošos apstākļos. Komisijai būtu būtiska nozīme šādas informācijas apkopošanā un izplatīšanā. Šāds risinājums nenodrošinātu ātru reaģēšanu, kas nepieciešama nenovēršamu draudu gadījumā. Tomēr pastāvētu iespēja turpmāk paplašināt KIBIT.

(2) **KIBIT būtu ātrās reaģēšanas sistēma (ĀRS), kas savienotu dalībvalstis un Komisiju.** Šāds risinājums palielinātu kritiskās infrastruktūras drošību, nodrošinot brīdināšanu tikai par tūlītējiem draudiem un trauksmēm. Šajā sakarā mērķis būtu veicināt ātru informācijas apmaiņu par iespējamiem draudiem KI īpašniekiem un apsaimniekotājiem. ĀRS neparedzētu izlūkdatu apmaiņu par ilgāku laikposmu. To izmantotu ātrai informācijas apmaiņai par tūlītējiem draudiem īpašai infrastruktūrai.

(3) **KIBIT būtu vairāku līmeņu saziņas/trauksmes sistēma, kas ietver divas atšķirīgas funkcijas:** a) ātrās reaģēšanas sistēma (ĀRS), kas savienotu dalībvalstis un Komisiju, un b) tāds forums ideju un paraugprakses par KIA apmaiņai KI īpašnieku un apsaimniekotāju atbalstam, kurā ietilpst ekspertu tīkls un elektronisko datu apmaiņas platforma.

Neatkarīgi no izvēlētā risinājuma, KIBIT papildinātu esošos tīklus, un tiktu veikti pienācīgi pasākumi, lai novērstu dublēšanos. Ilgtermiņā KIBIT varētu būt saistīts ar attiecīgajiem KI īpašniekiem un apsaimniekotājiem katrā dalībvalstī, izmantojot, piemēram, VKKI. Par trauksmi un paraugpraksi varētu informēt, izmantojot šo struktūru, kas būtu vienīgais dienests, kurš ir tieši saistīts ar Komisiju un tādējādi – ar visām pārējām dalībvalstīm. Dalībvalstis varētu izmantot savas esošās sistēmas, lai izveidotu savu valsts KIBIT veida tīklu, savienojot iestādes ar īpašiem īpašniekiem un apsaimniekotājiem. Ir svarīgi, lai šos valsts tīklus attiecīgās dalībvalsts KIA iestādes, kā arī īpašnieki un apsaimniekotāji varētu izmantot kā divpusēju saziņas sistēmu.

Tiks uzsākts pētījums, lai noskaidrotu jomu un tehniskās specifikācijas, kas nepieciešamas KIBIT turpmākajai saskarnei ar dalībvalstīm.

Jautājumi

Kādam vajadzētu būt KIBIT veidam, lai atbilstu EPKIA mērķiem?

Vai KI īpašniekiem un apsaimniekotājiem ir nepieciešams pieslēgums KIBIT?

9.2. Kopīga metodika

Dažādās dalībvalstīs atkarībā no dažādām situācijām ir dažādi trauksmes līmeņi. Pašlaik nav iespējams noteikt, vai, piemēram, „augsts" vienā dalībvalstī ir tas pats, kas „augsts" citā dalībvalstī. Šajā sakarā starptautiskām uzņēmējsabiedrībām var būt sarežģīti noteikt, kuri izdevumi par aizsardzības pasākumiem ir prioritāri. Tādēļ, iespējams, ir lietderīgi mēģināt saskaņot vai kalibrēt atšķirīgos līmeņus.

Katram apdraudējuma līmenim varētu atbilst gatavības līmenis, kad jāpiemēro vispārējie drošības pasākumi vispār un, ja vajadzīgs, jo īpaši klasificēti drošības pasākumi. Dalībvalstis, kas nevēlas izmantot konkrētu pasākumu, varētu īpašu draudu situācijā piemērot alternatīvus drošības pasākumus.

Varētu apsvērt kopīgu metodiku draudu, iespēju, risku un neaizsargātības identificēšanai un klasificēšanai un secinājumu veikšanai par to, cik iespējami, varbūtēji un nopietni ir draudi infrastruktūras iekārtas darbības pārtraukšanai. Tostarp tiktu veikta riska novērtēšana un prioritāšu noteikšana, saistībā ar ko riska gadījumus varētu definēt attiecībā uz to rašanās iespējamību, ietekmi un saistību ar citām riska jomām vai procesiem.

Jautājumi

Cik lielā mērā ir vēlams un lietderīgi saskaņot vai kalibrēt dažādos trauksmes līmeņus?

Vai būtu nepieciešama kopīga metodika draudu identificēšanai un klasificēšanai un secinājumu veikšanai par to, cik iespējami, varbūtēji un nopietni ir draudi?

9.3. Finansējums

Pamatojoties uz Eiropas Parlamenta iniciatīvu (jaunas budžeta pozīcijas izveide – izmēģinājuma projekts „Cīņa pret terorismu" 2005. gada budžetā), Komisija 15. septembrī pieņēma lēmumu piešķirt 7 miljonus euro, lai finansētu darbību kopumu, kas Eiropā uzlabos teroristu uzbrukumu novēršanu, gatavību un reaģēšanu uz tiem, tostarp tādās jomās kā seku pārvaldība, kritisko infrastruktūru aizsardzība, terorisma finansēšana, sprāgstvielas un vardarbīga radikalizēšanās. Vairāk nekā divas trešdaļas minētā budžeta ir paredzētas, lai sagatavotu nākamo Eiropas programmu kritiskās infrastruktūras aizsardzībai, to iespēju integrācijai un pilnveidei, kas nepieciešamas tādu starptautiski nozīmīgu krīžu novēršanai, ko var radīt teroristu draudi, un ārkārtas pasākumiem, kas var būt nepieciešami, lai vērstos pret šādiem uzbrukumiem vai nopietniem šādu uzbrukumu draudiem. Paredzams, ka minētā finansējuma nodrošināšanu turpinās 2006. gadā.

No 2007. gada līdz 2013. gadam līdzekļus piešķirs saistībā ar pamatprogrammu par drošību un brīvību nodrošināšanu. Šajā sakarā tiks iekļauta īpaša programma „Teroristu uzbrukumu novēršana, gatavība un reaģēšana uz tiem"; Komisijas priekšlikumā ir piešķirta summa EUR 137,4 miljonu apmērā, kas paredzēta, lai identificētu attiecīgās vajadzības un izstrādātu vienotus standartus kritiskās infrastruktūras aizsardzībai.

Programma nodrošinās Kopienas finansējumu projektiem, ko kritisko infrastruktūru aizsardzībai iesniegs valsts, reģionālās un vietējās pārvaldes iestādes. Galvenā uzmanība programmā ir veltīta aizsardzības vajadzību identificēšanai un informācijas sniegšanai saistībā ar vienotu standartu izstrādi, draudu un riska novērtējumiem, lai aizsargātu kritisko infrastruktūru vai izstrādātu īpašus ārkārtas rīcības plānus. Komisija izmantotu savas esošās zināšanas vai varētu palīdzēt finansēt pētījumus par savstarpēju atkarību īpašās nozarēs. Tādējādi galvenokārt dalībvalstis vai īpašnieki un apsaimniekotāji ir atbildīgi par to, lai uzlabotu savas infrastruktūras drošību saskaņā ar identificētajām vajadzībām. Programmā nav paredzēts finansēt kritiskās infrastruktūras aizsardzības uzlabošanu. Finanšu iestāžu sniegtos aizdevumus varētu izmantot infrastruktūras drošības uzlabošanai dalībvalstīs atkarībā no vajadzībām, kas identificētas, izmantojot programmu, un vienoto standartu ieviešanai. Komisija labprāt atbalstīs nozaru pētījumus, kas veikti, lai novērtētu finansiālās sekas, ko infrastruktūras drošības uzlabošana var radīt attiecīgajai nozarei.

Komisija finansē pētniecības projektus, lai atbalstītu kritiskās infrastruktūras aizsardzību drošības pētniecības sagatavošanas darbības jomā[2] (no 2004. līdz 2006. gadam), un ir paredzējusi nozīmīgākas darbības drošības izpētes jomā priekšlikumā Padomes un Eiropas Parlamenta Lēmumam par EK Septīto pētniecības pamatprogrammu (KOM(2005)119 galīgais)[3], kā arī priekšlikumā Padomes Lēmumam par īpašu programmu „Sadarbība", ar ko īsteno Septīto pamatprogrammu (KOM(2005)440 galīgais). Mērķtiecīgai izpētei ar nolūku sniegt praktiskas stratēģijas vai līdzekļus riska mazināšanai ir vislielākā nozīme, lai nodrošinātu ES kritisko infrastruktūru drošību vidējā termiņā vai ilgtermiņā. Visa veida drošības izpēti, tostarp šajā jomā, pārskatīs no ētikas viedokļa, lai nodrošinātu atbilstību Pamattiesību hartai. Prasības attiecībā uz izpēti pieaugs, vienīgi palielinoties savstarpējai atkarībai saistībā ar infrastruktūru.

Jautājumi

Kā jūs vērtējat šajā zaļajā grāmatā piedāvāto pasākumu īstenošanas izmaksas un ietekmi attiecībā uz pārvaldes iestādēm un ražotājiem? Vai uzskatāt, ka ir nodrošināta proporcionalitāte?

9.4. Novērtēšana un uzraudzība

EPKIA īstenošanas novērtēšana un uzraudzība paredz vairāku līmeņu procesu, kurā nepieciešams, lai tiktu iesaistītas visas ieinteresētās personas:

- **ES līmenī varētu ieviest salīdzinošās novērtēšanas mehānismu**, saistībā ar ko dalībvalstis un Komisija sadarbotos, novērtējot EPKIA īstenošanas vispārējo līmeni katrā dalībvalstī. Varētu sagatavot ikgadējus Komisijas progresa ziņojumus par EPKIA īstenošanu;

- **Komisija katru kalendāro gadu dalībvalstīm un citām iestādēm ziņotu par paveikto** Komisijas dienestu darba dokumentā;

---

2 Kredītu kopsumma 2004. un 2005. gada budžetā ir EUR 30 miljoni. Komisija ir ierosinājusi 2006. gada budžetā iekļaut summu EUR 24 miljonu apmērā, ko pašlaik izvērtē budžeta lēmējiestāde.

3 Komisijas budžeta projektā drošības un kosmosa izpētes darbībām saskaņā ar Septīto pamatprogrammu pētniecības, tehnoloģiju attīstības un demonstrējumu pasākumiem ir paredzēta summa EUR 570 miljonu apmērā (KOM(2005) 119 galīgais).

- **dalībvalstu līmenī VKKI, ievērojot savu jurisdikciju, katrā dalībvalstī varētu uzraudzīt EPKIA vispārējo īstenošanu, nodrošinot atbilstību valsts KIA programmai (-ām) un nozaru KIA programmām**, lai nodrošinātu to efektīvu īstenošanu, izmantojot gada ziņojumus Padomei un Komisijai.

EPKIA īstenošana būtu dinamisks process, ko pastāvīgi pilnveidotu un novērtētu, lai nodrošinātu tā atbilstību notiekošajām izmaiņām un izmantotu gūto pieredzi. Instrumenti, kas paredzēti EPKIA pārskatīšanai un jaunu pasākumu ierosināšanai nolūkā stiprināt kritiskās infrastruktūras aizsardzību, varētu ietvert salīdzinošās pārskatīšanas novērtējumus un dalībvalstu uzraudzības ziņojumus.

Dalībvalstu attiecīgo informāciju par EKI varētu darīt zināmu Komisijai, lai izstrādātu kopīgus neaizsargātības novērtējumus, seku pārvaldības plānus, vienotus standartus KI aizsardzībai, prioritāšu noteikšanai attiecībā uz izpētes darbībām un, ja vajadzīgs, regulēšanai un saskaņošanai. Šādu informāciju klasificētu un glabātu pilnīgā slepenībā.

Komisija varētu uzraudzīt dažādas dalībvalstu iniciatīvas, tostarp tās, kas paredz finansiālas sekas īpašniekiem un apsaimniekotājiem, kas pēc noteikta maksimālā termiņa nespēj atsākt pakalpojumu sniegšanu iedzīvotājiem.

Jautājums

Kāda veida novērtēšanas mehānisms būtu nepieciešams EPKIA? Vai iepriekš minētais mehānisms būtu pietiekams?

Atbildes jānosūta elektroniski līdz 2006. gada 15. janvārim uz šādu e-pasta adresi: **JLS-EPCIP@cec.eu.int**. Tās būs konfidenciālas, ja respondents skaidri nenoteiks, ka vēlas to publiskošanu; šādā gadījumā atbildes tiks publicētas Komisijas tīmekļa vietnē.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

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

Alert

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

Critical infrastructure protection (CIP)

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

Critical Information Infrastructure (CII):

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

Critical Information Infrastructure Protection (CIIP)

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

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

Contingency plan

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

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

Critical Information

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

Critical Infrastructure (CI)

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

There are three types of infrastructure assets:

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

Essential service

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

European critical infrastructure (ECI)

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

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

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

Impact

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

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

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

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

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

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

  - Interdependency (between other critical infrastructure elements).

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

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

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

Interdependency

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

Occurrence

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

Operator Security Plan

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

Prevention

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

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

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

Response

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

Risk

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

Threat

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

Vulnerability

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

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

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

ANNEX 3

OPERATOR SECURITY PLAN

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

Introduction)

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

Detailed part *(classified)*

– **Presentation of the operator**

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

– **Legal context**

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

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

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

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

– **Formalisation of security requirements**

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

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

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

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

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

– **Presentation and application**

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

– **Monitoring and updating**

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