EIROPAS KOPIENU KOMISIJA

Briselē, 20.10.2004
COM(2004) 702 galīgā redakcija

KOMISIJAS PAZIŅOJUMS
PADOMEI UN EIROPAS PARLAMENTAM

Kritisko infrastruktūru aizsardzība cīņā pret terorismu

SATURS

1. IEVADS 3

2. APDRAUDĒJUMS, KO RADA TERORISMS 3

3. EIROPAS KRITISKĀS INFRASTRUKTŪRAS 3

3.1. Kritisko infrastruktūru definējums 3

3.2. Drošības pārvaldība 5

4. POZITĪVI VĒRTĒJAMIE REZULTĀTI, KAS KOPIENAS LĪMENĪ GŪTI KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAS JOMĀ 6

5. ES KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAS SPĒJU NOSTIPRINĀŠANA 7

5.1. Eiropas programma kritisko infrastruktūru aizsardzībai 7

5.2. EPKIA īstenošana 8

5.3. EPKIA programmas mērķi un progresa rādītāji 9

TEHNISKAIS PIELIKUMS 10

1. IEVADS

Savā 2004. gada jūnija sanāksmē Eiropadome uzdeva Komisijai un Augstajam pārstāvim par pienākumu sagatavot vispārēju stratēģiju nolūkā nostiprināt kritisko infrastruktūru aizsardzību.

Pašreizējā paziņojumā sniegts pārskats par darbībām, kuras pašlaik Komisija veic kritisko infrastruktūru aizsardzības jomā, un ierosināti papildu pasākumi tam, lai nostiprinātu esošos instrumentus un rīkotos atbilstoši Eiropadomes norādījumiem.

2. APDRAUDĒJUMS, KO RADA TERORISMS

Varbūtība tam, ka var tikt īstenoti katastrofāli teroristu uzbrukumi, kas var skart kritiskās infrastruktūras, pieaug ar katru dienu. Uz kritisko infrastruktūru kontroles sistēmām vērsta uzbrukuma sekas var būt ļoti dažādas. Ir vispārēji pieņemts domāt, ka veiksmīgam kiberuzbrukumam uzpuru nav daudz vai arī to nav nemaz, taču tas varētu apturēt vitāli svarīgu infrastruktūru darbību. Piemēram, veiksmīgs kiberuzbrukums publiskajam telefonu komutācijas tīklam liegtu klientiem izmantot telefonu pakalpojumus, kamēr tehniķi atjaunotu un salabotu komutācijas tīklu. Uz ķīmisko iekārtu vai šķidrās dabas gāzes iekārtu kontroles sistēmām vērsts uzbrukums prasītu daudz vairāk upuru, kā arī izraisītu būtiskus materālus zaudējumus.

Kļūme vienā infrastruktūru daļā arī varētu izraisīt kļūmes citās, radot plašu kaskādes efektu. Pie līdzīga scenārija varētu novest sinerģisms dažādu infrastruktūru starpā. Tādējādi uz elektroapgādes iekārtām vērsts uzbrukums varētu izraisīt pārtraukumu elektropadevē, tāpat arī paralizēt ūdens attīrīšanas un pārvades iekārtas, ja nedarbojas šo iekārtu turbīnas un citas elektriskās ierīces.

Kaskādes efekts var izraisīt arī lielus zaudējumus, sakarā ar to, ka tiek apturēti daudzi pamatpakalpojumi. Biežie elektropadeves traucējumi Ziemeļamerikā un Eiropā pēdējo divu gadu laikā, norāda uz to, ko enerģijas jomā infrastruktūras nav drošas, un uz to, ka ir jāveic efektīvi pasākumi, lai novērstu/vai mazinātu sekas, ko rada nopietni traucējumi elektropadevē. Šāds kiberterorisma pielietojums var arī pastiprināt fiziska uzbrukuma sekas, piemēram, uzbrukums, ievietojot bumbu ēkā, kopā ar elektroapgādes vai telefonu pakalpojumu pārtraukumu uz laiku. Šajā gadījumā avārijas dienestu iejaukšanās tiek kavēta līdz brīdim, kad tiek atjaunota elektroapgāde vai komunikāciju sistēmas, savukārt tas var palielināt upuru skaitu un vairot paniku.

3. EIROPAS KRITISKĀS INFRASTRUKTŪRAS

3.1. Kritisko infrastruktūru definējums

Kritiskās infrastruktūras ir fiziskas iekārtas un informācijas tehnoloģijas, tīkli, pakalpojumi un līdzekļi, kas gadījumā, ja tie tiek iznīcināti vai ja to darbība tiek pārtraukta, var nopietni kaitēt iedzīvotāju veselībai, drošībai vai labklājībai un arī kavēt dalībvalstu valdību darbu. Kritiskās infrastruktūras ir daudzās tautsaimniecības nozarēs, tostarp tādās kā banku darbība un finanses, transports un apgāde, enerģija, pamatpakalpojumi, veselības aizsardzība, pārtikas apgāde un komunikācijas, kā arī administratīvie pamatpakalpojumi. Atsevišķus šo nozaru

kritiskos elementus nevar uzskatīt par "infrastruktūrām" tiešā nozīmē; patiesībā tie ir tīkli vai apgādes ķēdes, kas nodrošina kāda būtiska produkta piegādi vai kādu būtisku pakalpojumu. Piemēram, pārtikas vai ūdens apgāde mūsu lielākajās pilsētu teritorijās ir atkarīga no dažu izšķirīgi nozīmīgu iekārtu darbības, kā arī no tā, cik sekmīgi darbojas sarežģīts ražotāju, pārstrādātāju, izgatavotāju, izplatītāju un mazumtirgotāju tīkls.

Kritiskās infrastruktūras aptver šādus elementus:

- Energoietaises un tīkli (piem., elektroenerģijas, naftas un gāzes ražošanas, glabāšanas iekārtas un pārstrādes, pāvades un sadales sistēma);

- Komunikāciju un informācijas tehnoloģijas (piem., telekomunikācijas, apraides sistēmas, programmatūra, datoraparatūra un tīkli, tostarp Internets);

- Finanses (piem., bankas, vērtspapīri un ieguldījumi);

- Veselības aprūpe (piem., slimnīcas, veselības aprūpes iekārtas un asins bankas, laboratorijas un farmaceitiskie līdzekļi, meklēšanas un glābšanas, neatliekamās palīdzības dienesti);

- Pārtika (piem., drošums, ražošanas līdzekļi, vairumtirdzniecība un pārtikas rūpniecība);

- Ūdens (piem., rezerves, uzglabāšana, attīrīšana un tīkli);

- Transports (piem., lidostas, ostas, kombinētas transportsistēmas, dzelzceļa un pasažieru tranzīta tīkli, satiksmes kontroles sistēmas);

- Bīstamu preču ražošana, uzglabāšana un pārvadāšana (piem., ķīmisku, bioloģisku, radioloģisku vielu un kodolmateriālu ražošana, uzglabāšana un pārvadāšana);

- Pārvaldība (piem., pamatpakalpojumi, iekārtas, informāciju tīkli, līdzekļi un galvenie nacionālie objekti un pieminekļi)

Šīs infrastruktūras ir kā valsts sektora, tā privātā sektora pārziņā un īpašumā. Taču savā 2001. gada 10. oktobra Paziņojumā 574/2001 Komisija ir norādījusi: "Attiecīgajām valsts iestādēm ir jāuzņemas atbildība par to, lai tiktu stiprināti konkrēti drošības pasākumi sakarā ar uzbrukumiem, kas vērsti uz sabiedrību kopumā, nevis uz atsevišķu nozaru uzņēmumiem". Tādejādi valsts sektors ir aicināts veikt galvenos uzdevumus šajā sakarā.

Kritiskās infrastruktūras definējamas dalībvalstu līmenī un Eiropas līmenī, un šiem sarakstiem ir jābūt gataviem līdz 2005. gada beigām.

Eiropas kritiskās infrastruktūras ir cieši saistītas un cita no citas atkarīgas. Šo situāciju ir veicinājusi uzņēmumu koncentrācija, rūpnieciskā racionalizācija, tāda veida prakses kā, piemēram, ražošana atbilstoši iepriekš strikti noteiktai plūsmai, kā arī iedzīvotāju koncentrācija pilsētteritorijās. Eiropas kritiskās infrastruktūras ir kļuvušas daudz atkarīgākas no kopīgām informācijas tehnoloģijām, tostarp Interneta tīkla, kā arī no satelītu radio navigācijas un komunikācijām. Šajās savstarpēji saistītajās infrastruktūrās var rasties secīgas problēmas, kas savukārt var izraisīt negaidītus un arvien nopietnākus traucējumus pamatpakalpojumu nodrošināšanā. Šīs infrastruktūru savstarpējās saiknes un savstarpējā

atkarība ir iemesls tam, ka tās ir mazāk aizsargātas darbības traucējumu vai destruktīvu darbību gadījumā.

Būtu izpētāmi kritēriji, pēc kuriem infrastruktūras vai tās elementus uzskatām par kritiskiem. Šo kritēriju pamatā būtu jābūt arī kopīgām, kā arī pa nozarēm gūtām atziņām. Varētu izvirzīt trīs kritērijus potenciāli kritisku infrastruktūru identificēšanai:

- Darbības joma – kritisko infrastruktūru zaudējumu vērtē pēc tā, cik liels ir ģeogrāfiskais reģions, kas, iespējams, varētu tikt skarts – starptautiskas, valsts, provinces/teritoriālas vai vietējas nozīmes infrastruktūra.

- Varbūtēji izraisīto zaudējumu smaguma pakāpe – zaudējumu pakāpes var būt šādas - zaudējumu nav, minimāli, vidēji vai lieli zaudējumi. Turpmāk norādīti kritēriji, kurus varētu izmantot, lai novērtētu zaudējumu smagumu:

    (a) uz sabiedrību atstātās sekas (skarto personu skaits, nāves gadījumi, slimības, smagi savainojumi, evakuācija);

    (b) uz ekonomiku atstātās sekas (uz IKP atstātās sekas, saimniecisko zaudējumu apmērs un/vai produktiem vai pakalpojumiem nodarītais kaitējums);

    (c) uz vidi atstātās sekas (uz sabiedriskajām vietām un apkārtējo vidi atstātās sekas);

    (d) savstarpējā atkarība (attiecībā uz citām kritiskām infrastruktūrām);

    (e) politiskas sekas (ticība valdības spējām).

- Ietekme laikā – šis kritērijs nosaka, kurā brīdī kāda elementa zaudējums varētu izraisīt smagas sekas (t.i., tūlīt, pēc 24-48 stundām, vienas nedēļas, citi varianti).

Daudzos gadījumos psiholoģiskas dabas reakcija var saasināt citādi nenozīmīgus notikumus.

Pašreizējās pārmaiņas kritisko infrastruktūru aizsardzībā aptver tehniskais pielikums; tajā sniegts pārskats par to, ko Komisija uz šo brīdi ir veikusi katrā nozarē. Tas rāda, ka Komisija ir guvusi ievērojamu pieredzi šajā jomā.

3.2. Drošības pārvaldība

Nolūkā izanalizēt dalībvalstu kritiskās infrastruktūras un no tām atkarīgos elementus sakarā ar apdraudējumu, ko rada terorisms, un noteikt to drošumu ir vajadzīga informācija no vairākiem avotiem. Katrai nozarei un dalībvalstij būs jānosaka infrastruktūras, ko tā savā teritorijā uzskata par kritisku, pēc ES līmenī saskaņotas formulas un sadarbojoties ar organizācijām vai personām, kas ir atbildīgas par drošību.

Nav iespējams pasargāt visas infrastruktūras no visiem draudiem. Piemēram, elektrības pārvades tīkli ir pārāk apjomīgi, lai tos parargātu, tos apjožot vai uzraugot. Piemērojot riska pārvaldības metodes, varam koncentrēties uz vietām, kuras ir visvairāk apdraudētas, ņemot vērā apdraudējumu, to, cik lielā mērā infrastruktūras ir kritiskas, esošo aizsardzības līmeni un pieejamo seku mazināšanas stratēģiju efektivitāti, lai nodrošinātu darbības nepārtrauktību.

Drošības pārvaldība ir apzināts process, kas domāts tam, lai noteiktu risku un definētu un īstenotu darbības nolūkā samazināt risku līdz kādam noteiktam un pieņemamam līmenim ar pieņemamām izmaksām. Šīs pieejas pamatā ir riska noteikšana, novērtēšana un kontrole, lai nodrošinātu līmeni, kas ir samērīgs ar to, kāds ir noteikts.

Kritisko infrastruktūru aizsardzība (KIA) prasa konsekventas partnerattiecības, kuru pamatā ir sadarbība starp kritisko infrastruktūru īpašniekiem un apsaimniekotājiem un dalībvalstu iestādēm. Par riska pārvaldību fizisko iekārtu, apgādes ķēžu, informācijas tehnoloģiju un komunikāciju tīklu līmenī vispirms atbild īpašnieki un apsaimniekotāji.

Ir jāizplata brīdinājumi, ieteikumi un informācija, lai palīdzētu valsts un privātā sektora partneriem aizsargāt savas galvenās infrastruktūras. Gadās arī tā, ka sakarā ar specifisku teroristu uzbrukuma risku vai apdraudējumu ir vajadzīga tūlītēja rīcība. Šādā gadījumā dalībvalstu valdībām un attiecīgajai nozarei ir jārīkojas mērķtiecīgi un saskaņoti. Šavukārt ES pienākums būtu saskaņot vajadzīgās politiskās nostādnes, un, pamatojoties uz tām, partneriem sadarbojoties, definējami pasākumi katrā atsevišķā gadījumā.

Pat vislabākie plāni un likumi drošības pārvaldības jomā nelīdz, ja tos piemēro nepareizi. Pieredze rāda, ka neatkarīgas pārbaudes, ko Komisija veic, lai kontrolētu piemērojumu, ir vienīgais veids, kā efektīvi garantēt to, drošības prasības izpildītas pareizi.

4. POZITĪVI VĒRTĒJAMIE REZULTĀTI, KAS KOPIENAS LĪMENĪ GŪTI KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAS JOMĀ

Eiropieši vēlas, lai kritiskās infrastruktūras turpinātu darboties neatkarīgi no tā, kādas organizācijas īpašums tās ir vai kas ir to pārvaldītājorganizācija. Viņi uzskata, ka šajā ziņā atbildība vispirms ir jāuzņemas dalībvalstu valdībām un ES. Eiropieši sagaida sadarbību visu līmeņu valsts un privātā sektora īpašnieki un pārvaldītāji starpā, lai nodrošinātu, ka tie pakalpojumi, no kuriem viņi ir atkarīgi, turpinātu darboties.

Lai papildinātu valsts līmenī veiktos pasākumus, Eiropas Savienība jau ir noteikusi virkni likumdošanas pasākumu attiecībā uz obligātiem standartiem infrastruktūru aizsardzībā atbilstīgi dažādām ES politikām. Tas jo īpaši attiecas uz transportu, komunikācijām, enerģiju, arodveselību un darba drošības un veselības aizsardzības sektoriem. Jauns stimuls šiem pasākumiem bija nesenie uzbrukumi Amerikā un Eiropā; tie veicinās esošo pasākumu uzlabošanu vai paplašināšanu.

Gadu desmitiem saskaņā ar EURATOM līgumu veiktas pārbaudes, lai kontrolētu kodolmateriālu pareizu izmantošu. Aizsardzībā pret radiāciju ir daudz tiesību aktu, kas attiecas uz riskiem, kuri saistīti ar kodoliekārtu darbību un tādu avotu izmantošanu, kuros ir radioaktīvas vielas.

Starptautiskā transporta jomā Eiropas Savienība pieņēmusi tiesību aktus nolūkā īstenot vai nostiprināt nolīgumus, kas noslēgti starptautiskās organizācijās, kas regulē aviāciju un jūras transportu. Eiropas Savienība arī turpmāk īstenos un sekmēs savas darbības starptautiskā līmenī, un mudinās trešās valstis, kuras sadarbojas ar ES saimnieciskos jautājumos, īstenot šos nolīgumus. Dažām no tām ES ir sniegusi atbalstu, lai panāktu vienādu un noturīgu drošības līmeni ES un ārpus tās robežām.

Nākošais solis komunikāciju drošības nodrošināšanā ir Eiropas tīklu un informācijas drošības aģentūras (ETIDA) izveide. Turklāt tādos sektoros kā gaisa un jūras transporta drošība,

Komisijā izveidoti dienesti, kuru uzdevums ir kontrolēt to, kā dalībvalstīs piemēro tiesību aktus drošības jomā. Pateicoties šīm pārbaudēm var nonākt pie atskaites punktiem un panākt vienādu īstentojuma līmeni visā Eiropas Savienībā.

Informāciju attiecībā uz pašreizējām pārmaiņām kritisko infrastruktūru aizsardzības jomā aptver tehniskais pielikums; tajā sniegts īss pārskats pa nozarēm attiecībā uz to, kas uz šo brīdi paveikts Komisijā. Tas apliecina, ka Komisija ir guvusi ievērojamu pieredzi šajā jomā.

5. ES KRITISKO INFRASTRUKTŪRU AIZSARDZĪBAS SPĒJU NOSTIPRINĀŠANA

5.1. Eiropas programma kritisko infrastruktūru aizsardzībai

Ņemot vērā to, ka kritisko infrastruktūru skaits var būt liels, un visas tās ir savām individuālām iezīmēm, nav iespējams tās visas aizsargāt ar Eiropas līmeņa pasākumiem. Piemērojot subsidaritātes principu, Eiropai ir jākoncentrē savi pūliņi uz pārrobežu infrastruktūru aizsardzību, savukārt atbildība par pārējām būtu atstājama dalībvalstu ziņā, bet saskaņā ar kopēju sistēmu.

Daudzas direktīvas un regulas jau ir pieņemtas; tās paredz līdzekļus negadījumu atklāšanai, intervences plānu izstrādi sadarbībā ar civilo aizsardzību, regulāras mācības un skaidras attiecības starp dažādajiem intervences līmeņiem, valsts iestādēm, centrālajām organizācijām un neatliekamās palīdzības dienestiem. Tomēr vēl ļoti daudz jādara, lai nodrošinātu aizsardzību cita veida enerģijas ražošanas iekārtām, kas nav kodolenerģija. Kā uz to norāda tehniskais pielikums, kritisko infrastruktūru aizsardzības jomā pieņemtā *acquis communautaire* līmeņi ir atšķirīgi.

Vairumā no še iepriekš minētajām jomām darbs turpinās, un tiek īstenota sadarbība ar dalībvalstu ekspertiem un attiecīgajām tautsaimniecības nozarēm, lai apzinātu varbūtējus trūkumus un paredzētu veicamos korektīvos pasākumus (tiesiskus un citus). Ir izveidoti daudzi tīkli un drošības komitejas.

Katru gadu Komisija nāks klajā ar paziņojumu pārējām institūcijām nolūkā tās informēt par paveikto. Tajā pa nozarēm tiks izanalizēts tas, kādas bijušas pārmaiņas kopienas darbā attiecībā uz riska novērtēšanu, aizsardzības metožu izstrādi vai tiesiskām darbībām, ko īsteno vai ko ir paredzēts īstenot, lai ņemtu vērā ieteikumus. Vajadzības gadījumā Komisija šajā paziņojumā nāks klajā ar jauninājumiem un horizontāliem pasākumoiem, kas paredz saskaņošanu, koordināciju vai sadarbību. Šis paziņojums, kas aptvers visus pētījumus un pasākumus pa nozarēm, būs bāze Eiropas programmai kritisko infrastruktūru aizsardzībai (EPKIA).

Šai programmai būtu jākalpo par atbalstu dalībvalstu nozarēm un pārvaldēm visos līmeņos ES, tai pašā laikā respektējot individuālo atbildību un pienākumus. Pēc Komisijas domām, tīkls, kas aptver ES dalībvalstu speciālistus KIA jomā, varētu palīdzēt Komisijai izstrādāt šo programmu- šis brīdinājuma informācijas tīkls attiecībā uz kritiskajām infrastruktūrām (KIBIT) ir jāizveido pēc iespējas ātri 2005. gadā.

Tīkla izveidei būtu būtiski jāsekmē savstarpēja apmaiņa ar informāciju par kopīgiem apdraudējumiem un neaizsargātību, ar attiecīgiem pasākumiem un stratēģijām, kas ļauj mazināt risku, un tādejādi pasargāt kritiskās infrastruktūras. Dalībvalstīm savukārt būtu

jāgādā par to, lai informācija tiktu nosūta visiem attiecīgajiem pārvaldes departamentiem un organizācijām, tostarp neatliekamās palīdzības dienestiem un rūpniecības nozarēm, un tām, savukārt, izmantojot dalībvalstīs izveidoto kontaktu tīklu, jāinformē attiecīgo kritisko infrastruktūru īpašnieki un pārvaldītāji.

EPKIA ļautu izveidot pastāvīgu forumu nolūkā rast līdzsvaru starp konkurences ierobežojumiem, informācijas nozīmīguma un jūtīguma ierobežojumiem un priekšrocībām, ko sniedz daudz drošākas kritiskās infrastruktūras. Šajā procesā notiks tiešas apspriedes ar rūpniecības nozaru pārstāvjiem. Programma sekmēs to, ka partneriem tiks nosūta plašāka informācija par specifiska apdraudējuma situācijām, lai viņi varētu paredzēt pasākumus un sagatavoties sakarā ar varbūtējām sekām. Nekas nemainās attiecībā uz īpašnieku un pārvaldītāju atbildību, kuriem pašiem ir jāpieņem savi lēmumi un jāplāno savu līdzekļu aizsardzība.

Tad, ja nav pa nozarēm vai starptautiski pieņemtu standartu, Eiropas Standartizācijas komiteja (CEN) un citas standartizācijas organizācijas varētu palīdzēt šim tīklam, ierosinot vienādas pa nozarēm piemērojamas un visām attiecīgajām nozarēm pielāgotas drošības normas. Šādas normas būtu jāierosina arī starptautiskā līmenī, izmantojot ISO, lai ieviestu vienādus nosacījumus.

Ir jābūt uzmanīgiem, runājot par kritisko infrastruktūru apdraudējumiem, tostarp terorismu, lai izvairītos no nevajadzīga satraukumu ES iedzīvotājos, tostarp potenciālajos tūristos un ieguldītājos. Terorisma draudi ir pastāvīgi, bet politikas veidotāju uzdevums ir aicināt savus iedzīvotājus turpināt dzīvot pēc iespējas ierastu dzīvi. Tāpat jārūpējas, lai tiktu ievērotas tiesības uz privāto dzīvi gan ES, gan ārpus tās. Patērētājiem un uzņēmējiem ir jābūt pārliecinātiem par to, ka konfidenciālu informāciju izmanto pareizi un uzticami. Attiecīgai sistēmai būtu jāgarantē, ka klasificētā informācija tiek pārvaldīta pareizi un ka to nevar nesankcionēti izmatot vai izpaust.

Liela daļa ES un dalībvalstu kritisko infrastruktūru šķērso ES robežas. Cauruļvadi aptver veselus kontinentus; informācijas tehnoloģiju pareizai darbībai nepieciešami kabeļi ir ierakti dziļi okeānu dibenā utt. Tas nozīmē, ka starptautiskā sadarbība ir būtiska, lai izveidotu dinamiskas valsts līmeņa un starptautiskas partnerattiecības starp kritisko infrastruktūru īpašniekiem un pārvaldītājiem un trešo valstu valdībām, un jo īpaši ES tiešajiem piegādātājiem enerģētikas jomā.

5.2. EPKIA īstenošana

Kritisko infrastruktūru aizsardzība paredz to, ka aktīvi līdzdarbojas infrastruktūru īpašnieki un pārvaldītāji, reglamentējošās iestādes, profesionālās un nozaru organizācijas, dalībvalstis un Komisija. Pamatojoties uz dalībvalstu sadarbības partneru un, izmantojot tīklu, sniegto informāciju, EPKIA mērķis būs turpināt apzināt kritiskās infrastruktūras, analizēt to, cik lielā mērā tās ir neaizsargātas un savstarpēji atkarīgas, piedāvāt risinājumus to aizsardzībai un to sagatavotība ārkārtēju situāciju gadījumā. Šajā nolūkā jo īpaši ir jāpalīdz rūpniecības nozarēm, veicot riska novērtējumu, noteikt teroristu apdraudējumu un varbūtējās sekas. Dalībvalstu tiesībsargājošajām iestādēm un civilajai aizsardzībai savās plānošanas un informēšanas darbībās ir jāizmanto EPKIA.

Cieši sadarbojoties ar tīklu, Komisijas dienesti, veiks turpmākās darbības, jo īpaši tiesību aktu pieņemšana / informācijas izplatīšana. Sevišķo uzdevumu grupai, kurā ietilpst policijas un Eiropola vadītāji, būtu jāgādā par to, ka informācija par drošības līmeņiem, kā arī izlūkošanas

informācija tiek izplatīta dalībvalstu tiesībsargājošajām iestādēm. Savukārt šīm iestādēm ir jāsazinās ar kritisko infrastruktūru īpašniekiem un pārvaldītājiem un jāsniedz ieteikumi attiecībā uz apdraudējumiem, ko rada teroristi, un jāsekmē pretterorisma aizsardzības stratēģiju ieviešana.

Dalībvalstu valdības turpinās attīstīt un paplašināt datu bāzes attiecībā uz infrastruktūrām, kas ir nozīmīgas valsts līmenī, un būs atbildīgas par attiecīgu plānu izstrādāšanu, apstiprināšanu un pārbaudi, tādejādi nodrošinot pakalpojumu nepārtrauktību to teritorijā. Izstrādājot EPKIA, Komisija izteiks ierosinājumus par to, kādam būtu jābūt šādas datu bāzes obligātajam saturam un formātam, un kādā veidā tām jābūt savstarpēji saistītām.

Dalībvalstu valdībām būtu arī turpmāk jāsūta kritisko infrastruktūru īpašniekiem un pārvaldītājiem (kā arī citām dalībvalstīm, pēc vajadzības) svarīgākā izlūkošanas informācija un brīdinājumi, kā arī norādījumi tam, kā viņiem saskaņā ar noteikumiem ir jārīkojas katrā apdraudējuma/trauksmes situācijas līmenī.

Kritisko infrastruktūru īpašnieki un pārvaldītāji pienācīgi pasargās savus līdzekļus, ieviešot savus plānus drošības jomā un regulāri īstenojot pārbaudes, mācības, novērtējumus un plānus. Dalībvalstīm vispārēji jākontrolē process, savukārt Komisijai jānodrošina tā vienāds īstenojums visā Eiropas Savienībā, izmantojot attiecīgas pārbaudes sistēmas.

5.3. EPKIA programmas mērķi un progresa rādītāji

EPKIA programmas mērķis un Komisijas uzdevums būtu nodrošināt pienācīgus un vienādus aizsardzības līmeņus, līdz minimumam samazināt kļūmes un visai ES sniegt pārbaudītus tūlītējas rīcības līdzekļus. EPKIA pastāvīgi mainīsies; tā regulāri tiks izvērtēta atkal un atkal, atkarībā no tā, kā mainīsies problēmas un neatrisinātie jautājumi Kopienā.

Sekmes tiks novērtētas pēc šādiem elementiem:

- ar kritiskajām infrastruktūrām saistītā arsenāla apzināšana un izstrāde, ko, aptverot savu valsts teritoriju, dalībvalstis veic saskaņā ar prioritātēm EPKIA programmā;

- nozaru uzņēmumu sadarbība savā starpā un ar savu valdību, lai dalītos informācijā un mazinātu risku, ka var tikt piedzīvoti negadījumi, kas var radīt plašus vai ilgstošus kritisko infrastruktūru darbības traucējumus;

- Eiropas Kopiena definē kopēju stratēģiju kritisko infrastruktūru drošības problēmas risināšanā, sadarbojoties visām iesaistītajām valsts un privātajām personām.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

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

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

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.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has 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.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

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.