EUROOPA ÜHENDUSTE KOMISJON

Brüssel 20.10.2004
KOM(2004) 702 lõplik

KOMISJONI TEATIS
NÕUKOGULE JA EUROOPA PARLAMENDILE

Kriitilise infrastruktuuri kaitse terrorismivastases võitluses

SISUKORD

1. SISSEJUHATUS 3
2. OHT 3
3. EUROOPA KRIITILISED INFRASTRUKTUURID 3
3.1. Mis on kriitiline infrastruktuur 3
3.2. Julgeoleku haldamine 5
4. EDU KRIITILISE INFRASTRUKTUURI KAITSMISES LIIDU TASANDIL 6
5. ELi KRIITILISE INFRASTRUKTUURI KAITSMISE VÕIME SUURENDAMINE .. 7
5.1. Euroopa kriitilise infrastruktuuri kaitse programm 7
5.2. Euroopa kriitilise infrastruktuuri kaitse programmi rakendamine 8
5.3. Euroopa kriitilise infrastruktuuri kaitse programmi eesmärgid ja progressi näitajad 9
TEHNILINE LISA 10

1. SISSEJUHATUS

Euroopa Ülemkogu 2004. aasta juuni kohtumisel paluti komisjonil ja kõrgel esindajal ette valmistada üldine strateegia kriitilise infrastruktuuri kaitsmiseks.

Käesolev teatis annab ülevaate meetmetest, mida komisjon on praegu kriitilise infrastruktuuri kaitseks võtnud, ja pakub välja lisameetmed, et tugevdada olemasolevaid vahendeid ja tagada vastavus Euroopa Nõukogu poolt antud volitustele.

2. OHT

Kriitilisi infrastruktuure mõjutava katastroofilise terrorirünnaku oht suureneb. Rünnaku tagajärjed kriitilise infrastruktuuri tööstuslikele kontrollisüsteemidele võivad olla väga erinevad. Tavaliselt arvatakse, et edukas küberrünnak põhjustab väheseid või mitte üldse inimkaotusi, kuid võib põhjustada olulise infrastruktuuriteenuse kadumise. Näiteks edukas rünnak avalikule telekommutaatorvõrgule võib kliendid ilma jätta telefoniteenusest sel ajal, kui tehnikud kommutaatorvõrku uuesti seadistavad ja parandavad. Rünnak keemia- või loodusliku gaasi rajatise kontrollisüsteemidele võib viia ulatuslikuma inimkaotusteni ning oluliste füüsiliste kahjustusteni.

Teist tüüpi katastroofiline infrastruktuuri rike võib esineda siis, kui osa infrastruktuurist viib teiste osade riketeni, põhjustades ulatusliku lumepalliefekti. Selline rike võib tekkida infrastruktuuri tööstuste omavahelise koosmõju tõttu. Lihtsaks näiteks on rünnak elektrimajandusele, milles katkeb elektri jaotamine, samuti tekivad häired reoveepuhastites ja veevõrgus, sest välja võivad lülituda turbiinid ja teised elektriaparaadid neis rajatistes.

Lumepalliefekti tagajärjel sündmused võivad samuti olla väga kahjustavad, põhjustades ulatuslikku rajatiste töötamast lakkamist. Elektrikatkestused Põhja-Ameerikas ja Euroopas viimase kahe aasta jooksul on tõestanud energiainfrastruktuuride haavatavust ja sellest tulenevalt vajadust leida tõhusaid meetmeid suuremast elektrivarustuse katkemisest tingitud tagajärgede vältimiseks või leevendamiseks. Küberterrorismi kasutamine võib samuti põhjustada füüsilise rünnaku toime võimendumist. Selle näiteks võib olla tavaline pommirünnak ehitisele, mis on kombineeritud ajutise elektri- või telefoniteenuse puudumisega. Tulemusena tekkiv hädaolukorrale reageerimise halvenemine kuni varuelektri- või –sidesüsteemide kohale toomiseni ja kasutama hakkamiseni võib suurendada inimkaotuste hulka ja paanikat.

3. EUROOPA KRIITILISED INFRASTRUKTUURID

3.1. Mis on kriitiline infrastruktuur

Kriitilised infrastruktuurid koosnevad nendest füüsilistest ja infotehnoloogia rajatistest, võrkudest, teenustest ja ressurssidest, millel häirimisel või hävitamisel on tugev mõju kodanike tervisele, ohutusele, julgeolekule või majanduslikule heaolule või liikmesriikide valitsuste tõhusale toimimisele. Kriitilised infrastruktuurid hõlmavad paljusid majandussektoreid, kaasa arvatud pangandus ja rahandus, transport ja turustamine, energia, kommunaalmajandus, tervishoid, toiduga varustamine ja side, samuti ka valitsuse võtmeteenistused. Mõningad kriitilised elemendid nendes sektorites pole rangelt võttes

„infrastruktuur", kuid on tegelikult võrgud või tarneahelad, mis toetavad elutähtsate toodete või teenuste laialijagamist. Näiteks on toidu- või veevarustus meie suuremates linnastunud piirkondades sõltuv teatud võtmerajatistest, kuid samuti tootjate, töötlejate, turustajate ja jaemüüjate komplekssest võrgust.

Kriitiliste infrastruktuuride hulka kuuluvad:

- Energiarajatised ja võrgud (st elektrienergia, nafta ja gaasi tootmine, ladustamisrajatised ja töötlemistehased, edastamis- ja jaotussüsteem)
- Side ja infotehnoloogia (st telekommunikatsioon, edastamissüsteemid, tarkvara, riistvara ja võrgud, kaasa arvatud Internet)
- Rahandus (st pangandus, väärtpaberid ja investeeringud)
- Tervishoid (st haiglad, tervishoiu- ja verega varustamise rajatised, laborid ja ravimid, otsimis-, pääste- ja kiirabiteenistused)
- Toit (st ohutus, tootmisvahendid, hulgimüük ja toiduainetööstus)
- Vesi (st tammid, hoidmine, puhastamine ja võrgud)
- Transport (st lennujaamad, sadamad, ühendveorajatised, raudtee- ja massitransiidivõrgud, liikluse kontrollisüsteemid)
- Ohtlike kaupade tootmine, ladustamine ja transport (st keemilised, bioloogilised, radioloogilised ja tuumamaterjalid)
- Valitsus (st kriitilised teenistused, rajatised, infovõrgud, ressursid ning rahvuslikud võtmekohad ja monumendid)

Neid infrastruktuure omavad ja käitavad nii avalik kui erasektor. 10. oktoobri 2001. aasta teatises 574/2001 deklareeris komisjon: „Teatud julgeolekumeetmeid peab pärast ühiskonna kui terviku, kuid mitte tööstuse vastaseid rünnakuid tugevdama riik". Seepärast on põhiline roll avalikul sektoril.

Kriitilised infrastruktuurid tuleb määratleda liikmesriikide tasandil ja Euroopa tasandil ning vastavad nimekirjad koostada 2005. aasta lõpuks.

Euroopa kriitilised infrastruktuurid on omavahel tugevalt ühendatud ja üksteisest sõltuvad. Ettevõtete konsolideerumine, tööstuse ratsionaliseerimine, tõhusad äritavad, näiteks tootmine viimasel hetkel, ja rahvastiku kontsentratsioon linnastunud piirkondades on kõik seda olukorda soodustanud. Euroopa kriitilised infrastruktuurid on muutunud rohkem sõltuvaks tavalistest infotehnoloogiatest, kaasa arvatud Internet ja kosmosepõhine raadio-navigatsioon ja side. Probleemid võivad tulvata läbi nende omavahel sõltuvate infrastruktuuride, põhjustades ootamatuid ja üha tõsisemaid elutähtsate teenuste häireid. Omavahel ühendatus ja sõltuvus muudab need infrastruktuurid haavatavamaks häirete või hävitamise suhtes.

Tuleb uurida kriteeriume selliste faktorite määramiseks, mis muudavad konkreetse infrastruktuuri või infrastruktuuri elemendi kriitiliseks. Need valikukriteeriumid peavad

samuti põhinema sektori ja kollektiivsel kogemusel. Võib välja pakkuda kolm faktorit potentsiaalse kriitilise infrastruktuuri määratlemiseks:

- Ulatus – kriitilise infrastruktuuri elemendi kaotust hinnatakse geograafilise ala ulatuse alusel, mida mõjutab selle kaotus või kättesaadamatus – rahvusvaheline, siseriiklik, piirkondlik/territoriaalne või kohalik.

- Suurus – mõju või kaotuse suurust saab hinnata kui puuduvat, minimaalset, keskmist või suurt. Potentsiaalse suuruse hindamise kriteeriumide hulka kuuluvad:

    (a) Mõju elanikkonnale (mõjutatud elanikkonna suurus, inimohvrid, meditsiinilised haigused, rasked vigastused, evakuatsioon);

    (b) Mõju majandusele (mõju SKT-le, olulised majanduslikud kaotused ja/või toodete ja teenuste halvenemine);

    (c) Mõju keskkonnale (mõju avalikule ja ümbritsevale paikkonnale);

    (d) Omavaheline sõltuvus (teiste kriitiliste infrastruktuuri elementidega);

    (e) Poliitiline mõju (usaldus valitsuse suutlikkuse vastu).

- Aja toime – see kriteerium määrab ära, millisel hetkel võib elemendi kaotusel olla tõsine mõju (st kohene, 24-–48 tundi, üks nädal, muu).

Paljudel juhtudel võivad siiski psühholoogilised mõjud eskaleerida muus osas ebaolulisi sündmusi.

Praegused kriitilise infrastruktuuri kaitse arengud on dokumenteeritud tehnilises lisas, mis annab sektorite alusel ülevaate komisjoni senistest saavutustest. Nad näitavad, et komisjon on omandanud olulise kogemuse sellel alal.

3.2. Julgeoleku haldamine

Mitmetest allikatest pärinev informatsioon on vajalik ohu-, vahejuhtumi- ja haavatavusanalüüsi läbiviimiseks liikmesriikide kriitiliste infrastruktuuride ja nende sõltuvuste osas. Iga sektor ja liikmesriik peab kindlaks määrama nende jaoks kriitilise infrastruktuuri oma jurisdiktsiooni all vastavalt ELi ühtlustatud valemile ning organisatsioonid ja isikud, kes vastutavad julgeoleku eest.

Mitte kõiki infrastruktuure ei saa kaitsta iga ähvarduste eest. Näiteks elektri- ja ülekandekandevõrgud on liiga suured aiaga ümberpiiramiseks või valvamiseks. Rakendades riskihaldamise tehnikaid saab tähelepanu keskendada kõige suurema riskiga aladele, arvestades ohtu, suhtelist kriitilisust, olemasolevat turbetaset ja olemasolevate leevendamisstrateegiate tõhusust äri järjepidevusele.

Julgeoleku haldamine on teadlik riski mõistmise ja tegevuste üle otsuse tegemise ja nende rakendamise protsess, et vähendada riski kindlaksmääratud tasemeni, mis on vastuvõetav riski tase vastuvõetava maksumuse puhul. Seda lähenemist iseloomustavad riskide identifitseerimine, mõõtmine ja kontrollimine tasemeni, mis vastab määratud tasemele.

Kriitilise infrastruktuuri kaitse vajab järjepidevat koostöösuhet kriitilise infrastruktuuri omanike ja operaatorite ning liikmesriigi võimude vahel. Vastutus riskihaldamise eest füüsilistes rajatistes, varustusahelates, infotehnoloogias ja sidevõrkudes kuulub peamiselt omanikele ja operaatoritele.

Tuleb anda hoiatusi, nõuandeid ja informatiivseid märkusi, et aidata avaliku ja erasektori sidusrühmadel kaitsta võtmetähtsusega infrastruktuurisüsteeme. Aeg-ajalt võivad esile kerkida konkreetsed riskid või terrorirünnaku ähvardused, mis nõuavad kohest reageerimist. Neil juhtudel on liikmesriikide valitsustelt ja tööstuselt nõutav hästi koordineeritud operatiivselt keskendatud vastus. Neil juhtudel peab EL koordineerima vajalikke poliitilisi vastuseid ja sel alusel lepitakse ükshaaval kokku sidusrühmadega detailsetes toetuse korraldamise küsimustes.

Isegi kõige paremad julgeoleku haldamise plaanid ja õigusaktid nende jõustamiseks pole midagi väärt ilma õige täideviimiseta. Kogemused näitavad, et sõltumatud komisjoni julgeolekuinspektsioonid on ainuke tõhus vahend turvanõuete korrektse täitmise tagamiseks.

4. EDU KRIITILISE INFRASTRUKTUURI KAITSMISES LIIDU TASANDIL

Eurooplased ootavad, et kriitilised infrastruktuurid jätkaksid talitlemist sõltumata sellest, millised organisatsioonid omavad või käitavad nende komponente. Nad ootavad, et liikmesriikide valitsused ja EL mängiksid juhtivat osa selle tagamisel. Nad ootavad valitsustelt ja erasektori omanike ja operaatorite kõigilt tasanditelt koostööd, et tagada selliste teenuste järjepidevus, millest eurooplased sõltuvad.

Lisaks meetmetele, mida on rakendatud siseriiklikul tasandil, on Euroopa Liit võtnud mitmeid õiguslikke meetmeid minimaalsete standardite kindlaksmääramiseks infrastruktuuri kaitse jaoks erinevate ELi poliitikate raames. Eriti tähelepandav on see transpordi-, side-, energia-, töötervishoiu ja -ohutuse ning rahvatervise sektoris. Tegevust on kiirendatud pärast hiljutisi rünnakuid Ameerikas ja Euroopas. Need viivad olemasolevate meetmete edasisele paranemisele ja laienemisele.

Aastakümnete jooksul on läbi viidud inspektsioone EURATOMi asutamislepingu raames, et kontrollida tuumamaterjalide õiget kasutamist. Kiirguskaitse alal on olemas olulisel määral õigusakte, mida kohaldatakse rajatiste käitamise ja radioaktiivsete ainete allikate kasutamise riskide suhtes.

Rahvusvahelise transpordi alal võttis Euroopa Liit vastu õigusakti, mis rakendab või tugevdab rahvusvaheliste juhtorganite lepinguid lennundus- ja merendussektoris. Euroopa Liit jätkab rahvusvahelisel tasandil nende tegevuse toetamist ja selles aktiivset osalemist. See julgustab kolmandaid riike, kes on majandussuhetes ELga, neid lepinguid rakendama. Liit on mõnele neist andnud teatud abi, eesmärgiga saavutada homogeenne ja pidev julgeolekutase ELi piirides ja väljaspool seda.

Edasiseks sammuks on selliste agentuuride nagu Euroopa Võrgu- ja Infoturbe Amet (ENISA - *European Network and Information Security Agency*) loomine sideturbe alal. Lisaks on sektorites, nagu lennundus ja merendus, loodud komisjonisisesed järelevalvetalitused, et kontrollida julgeolekualaste õigusaktide rakendamist liikmesriikide poolt. Need järelevalvetalitused loovad vajaliku võrdluspunkti, mis tagab liidus võrdse rakendamise taseme.

Praegused kriitilise infrastruktuuri kaitse arengud on dokumenteeritud tehnilines lisas, mis annab sektorite alusel ülevaate senistest komisjoni saavutustest. Nad näitavad, et komisjon on omandanud olulise kogemuse sellel alal.

5. ELI KRIITILISE INFRASTRUKTUURI KAITSMISE VÕIME SUURENDAMINE

5.1. Euroopa kriitilise infrastruktuuri kaitse programm

Arvestades potentsiaalsete kriitiliste infrastruktuuride suurt arvu ja nende iseärasusi, on võimatu neid kõiki kaitsta meetmetega Euroopa tasandil. Subsidiaarsuse põhimõtet kasutades peab Euroopa keskendama oma jõupingutused piiriülest mõju omavate infrastruktuuride kaitsele ja jätma teised liikmesriikide vastutada, kuid seda ühises raamistikus.

On olemas hulgaliselt direktiive ja määrusi, mis kehtestavad vahendid õnnetuste avastamiseks, sekkumisplaanide loomiseks koostöös kodanikukaitsega, regulaarseteks õppusteks ja selgeteks ühendusteks erinevate sekkumistasandite, avaliku võimkonna, tsentraalsete organisatsioonide ja kiireloomuliste teenuste vahel. Teiselt poolt on palju teha energiarajatiste kaitse osas (v.a tuumaenergiarajatised). Nagu näha tehnilines lisas, on olemas erinevas arenguastmes liidu õigustik kriitiliste infrastruktuuride kaitse kohta.

Enamikus ülalmainitud valdkondades jätkub töö ning on loodud koostöö liikmesriikide ekspertidega ja asjaomaste majandussektoritega, et kindlaks teha võimalikud vajakajäämised ja vajalikud korrektiivsed meetmed (seadusandlikud või muud). On loodud palju võrke ja julgeolekukomiteesid.

Komisjon raporteerib edusammudest teistele institutsioonidele igal kalendriaastal teatises. Ta analüüsib iga sektori jaoks arenguid riski hindamises, kaitsetehnikate väljatöötamises või käimasolevates/kavandatavates õigusalastes tegevustes, et saada neilt nõu. Lisaks pakub komisjon selles teatises vajadusel välja uuendused ja horisontaalsed organisatsioonilised meetmed, mille puhul on vajalik ühtlustamine, koordineerimine või koostöö. See teatis, mis ühendab kõiki sektorite analüüse ja meetmeid, kujutab endast alust Euroopa kriitilise infrastruktuuri kaitse programmile (EPCIP - *European Programme for Critical Infrastructure Protection*).

Selline programm püüab aidata tööstust ja liikmesriikide valitsusi kõigil tasanditel ELs, austades samas individuaalseid volitusi ja vastutust. Komisjonil arvab, et võrk, mis ühendab EL liikmesriikide kriitilise infrastruktuuri kaitse spetsialiste, saab aidata komisjonil programmi ette valmistada – see kriitilise infrastruktuuri hoiatusinfovõrk (CIWIN - *Critical Infrastructure Warning Network)* tuleb 2005. aastal võimalikult varakult üles seada.

Võrgu ülesseadmine peab olema abiks peamiselt selleks, et soodustada infovahetust jagatavate ohtude ja haavatavuste kohta ning sobilike meetmete ja strateegiate kohta riski vähendamiseks kriitilise infrastruktuuri kaitse puhul. Seepärast kontrollivad liikmesriigid omakorda, et asjassepuutuv informatsioon edastataks kõigile asjaomastele valitsusasutustele ja agentuuridele, kaasa arvatud hädaabiteenistuste organisatsioonidele, informeerides vastava tööstussektori organeid nii, et nemad omakorda informeeriksid vastavaid kriitilise infrastruktuuri omanikke ja operaatoreid liikmesriikides loodud kontaktvõrgu kaudu.

Euroopa kriitilise infrastruktuuri kaitse programm soodustab käimasolevat foorumit, kus konkurentsi piiranguid, kohustusi ja informatsiooni tundlikkust saab tasakaalustada turvalisema kriitilise infrastruktuuri poolt pakutavate hüvedega. Selle protsessi käigus konsulteeritakse tihedalt tööstusega. See aitab partneritele pakkuda rohkem informatsiooni konkreetsete ohusituatsioonide kohta, mis võimaldab neil võtta meetmeid potentsiaalsete tagajärgedega hakkama saamiseks. Omanike ja operaatorite vastutus teha omaenda otsuseid ja plaane oma ressursside kaitsmiseks ei muutu.

Kui pole olemas sektori standardeid või kui rahvusvahelisi norme pole veel kehtestatud, võivad Euroopa Standardikomitee (CEN - *European Committee for Standardization*) ja teised asjaomased standardiorganisatsioonid võrku abistada ja pakkuda välja ühetaolisi sektori ja kohandatud julgeolekustandardeid kõigi huvitatud harude ja sektorite jaoks. Sellised standardid tuleb välja pakkuda ka rahvusvahelisel tasandil ISO kaudu, et luua selles osas võrdne mänguruum.

Siseriiklikele kriitilise infrastruktuuri julgeolekuohtudele , kaasa arvatud terrorismile viidates tuleb olla ettevaatlik, et vältida asjatut muret nii ELs endas kui ka potentsiaalsete turistide ja investorite jaoks. Terrorism on pidev oht, kuid see on poliitikategijate ülesandeks julgustada kõiki oma eluga edasi minema nii häirimatult kui võimalik. Samuti tuleb olla hoolikas, et tagada austus eraelu puutumatuse vastu nii liidu sees kui väljaspool seda. Tarbijatel ja operaatoritel peab olema kindlus, et informatsiooni kasutatakse korrektselt, konfidentsiaalselt ja usaldusväärselt. On vajalik, et olemas oleks sobiv raamistik selle tagamiseks, et salastatud informatsiooni hallataks korrektselt ja kaitstaks seda loata kasutamise või avaldamise eest.

Suur osa nii ELi kui liikmesriikide kriitilisest infrastruktuurist ületab ELi piire. Torujuhtmed ulatuvad üle kontinentide, infotehnoloogia jaoks elulised kaablid on uputatud sügavale ookeanide põhja, jne. See tähendab, et rahvusvaheline koostöö on oluliseks komponendiks kestvate dünaamiliste rahvuslike ja rahvusvaheliste partnerluste loomisel kriitilise infrastruktuuri omanike/operaatorite ja kolmandate riikide valitsuste vahel, eriti liidu otseste energiatarnijatega.

5.2. Euroopa kriitilise infrastruktuuri kaitse programmi rakendamine

Kriitilise infrastruktuuri kaitse nõuab infrastruktuuri omanike ja operaatorite, seadusandjate, professionaalsete organite ja tööstusliitude ning liikmesriikide ja komisjoni aktiivset osalemist. Põhinedes liikmesriikide liidestelt ja võrgust saadud informatsioonil, on Euroopa kriitilise infrastruktuuri kaitse programm eesmärkideks kriitilise infrastruktuuri identifitseerimise jätkamine, haavatavuse ja omavahelise sõltuvuse analüüsimine ning lahenduste pakkumine kõigi ohtude eest kaitsmiseks ja nendeks valmistumiseks. See sisaldab tööstussektorite abistamist ohtude ja tagajärgede muutujate mõistmisel nende riskihinnangutes. Liikmesriikide õiguskaitseorganid ja kodanikukaitsemehhanism peavad tagama, et Euroopa kriitilise infrastruktuuri kaitse programm oleks nende planeerimise ja teadlikkuse tõstmise lahutamatu osa.

Lähedases koostöös võrguga aitavad komisjoni teenistused välja töötada edasisi tegevusi, mis peaksid koosnema õigusaktide vastuvõtmises ja/või informatsiooni jagamises. Politseijuhtide töökonnal ja Europolil on oma roll vastavate julgeolekutasemete ja luureinformatsiooni jaotamisel liikmesriikide õiguskaitseorganitele, kes omakorda peavad nõustama ja ühendust pidama kriitilise infrastruktuuri omanikega ja operaatoritega olulise ohuinformatsiooni osas, aitama, pakkudes nõuandeid kaitse kohta, ja töötama välja kaitsvaid turvastrateegiaid terrorismivastaseks võitluseks.

Liikmesriikide valitsused jätkavad ja/või arendavad ja säilitavad rahvuslikult olulise kriitilise infrastruktuuri andmebaase ning vastutavad vastavate plaanide arendamise, kinnitamise ja auditi eest, et tagada teenuste järjepidevus nende jurisdiktsiooni all. Euroopa kriitilise infrastruktuuri kaitse programmi koostades esitab komisjon ettepanekud, milline peab olema selliste andmebaaside minimaalne sisu ja formaat ja kuidas need peavad olema omavahel ühendatud.

Liikmesriikide valitsused jätkavad omakorda kriitilise infrastruktuuri omanike ja operaatorite informeerimist (nagu vajadusel ka teisi liikmesriike) asjassepuutuvatest luureandmetest ja hoiatustest nagu ka kokkulepitud reageerimisest, mida oodatakse iga ohu/hoiatuse taseme puhul sidusrühmadelt.

Kriitilise infrastruktuuri omanikud ja operaatorid tagavad oma ressursside adekvaatse turvalisuse, rakendades aktiivselt oma turvaplaane ja viies läbi regulaarseid inspektsioone, õppusi, hindamisi ja planeerimisi. Liikmesriigid peavad juhtima üldist protsessi, samas kui komisjon peab tagama kogu liidus ühetaolise rakendamise koos piisavate kontrollisüsteemidega.

5.3. Euroopa kriitilise infrastruktuuri kaitse programmi eesmärgid ja progressi näitajad

Euroopa kriitilise infrastruktuuri kaitse programmi eesmärgiks ja komisjoni kohustuseks on tagada, et oleksid olemas kriitilise infrastruktuuri kaitsejulgeoleku adekvaatsed ja ühetaolised tasemed, minimaalsed üksikud punktid, kus on võimalikud rikked, ning kiired, testitud taastumismehhanismid kogu liidus. Euroopa kriitilise infrastruktuuri kaitse programm on jätkuv protsess ja on vajalik regulaarne ülevaatamine, et hoida end kursis liidus esinevate küsimuste ja probleemidega.

Edukust mõõdetakse:

- Liikmesriikide valitsuste poolt kriitiliste infrastruktuuride määratlemise ja neist nimekirja koostamisega oma jurisdiktsiooni all vastavalt EPCIP prioriteetidele;

- Sektorites ja valitsusega koostööd tegevate ettevõtetega, kes jagavad informatsiooni ja vähendavad intsidentide tõenäosust, mis põhjustavad ulatuslikke ja pikaajalisi kriitiliste infrastruktuuride katkemisi;

- Euroopa Liit on otsustanud luua ühetaolise lähenemise kriitiliste infrastruktuuride julgeoleku rikkumistele koostöös kõigi avalike ja erasektori pooltega.

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.