EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 20.10.2004
KOM(2004) 702 lopullinen

KOMISSION TIEDONANTO
NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE

Kriittisen infrastruktuurin suojelu terrorismin torjunnassa

SISÄLLYSLUETTELO

1. JOHDANTO

Kesäkuussa 2004 kokoontunut Eurooppa-neuvosto pyysi komissiota ja korkeaa edustajaa laatimaan yleisstrategian kriittisen infrastruktuurin suojelemiseksi.

Tässä tiedonannossa luodaan katsaus komission tämänhetkisiin toimenpiteisiin kriittisen infrastruktuurin suojelun alalla ja ehdotetaan lisätoimenpiteitä nykyisten välineiden vahvistamiseksi ja Eurooppa-neuvoston toimeksiantojen toteuttamiseksi.

2. UHKA

Kriittiseen infrastruktuurin vaikuttavien katastrofaalisten terrori-iskujen mahdollisuus kasvaa. Kriittisen infrastruktuurin teknisiin ohjausjärjestelmiin kohdistuvan hyökkäyksen seuraukset voisivat olla hyvin moninaiset. On yleinen olettamus, että onnistunut tietoverkkohyökkäys aiheuttaisi vähän tai ei ollenkaan kuolonuhreja, mutta voisi johtaa tärkeän infrastruktuuripalvelun menettämiseen. Esimerkiksi onnistunut hyökkäys yleiseen puhelinverkkoon voisi estää asiakkaita käyttämästä puhelinta kunnes teknikot ovat saaneet verkon korjatuksi. Hyökkäys kemiallisia aineita valmistavan tuotantolaitoksen tai nestemäistä kaasua käsittelevän laitoksen ohjausjärjestelmiin voisi johtaa suurempiin ihmishenkien menetyksiin ja merkittäviin aineellisiin vahinkoihin.

Katastrofaalisia infrastruktuurihäiriöitä voi syntyä myös silloin, kun yksi infrastruktuurin osa johtaa häiriöihin sen muissa osissa aiheuttaen pitkän ketjureaktion. Tällainen häiriö voi olla seurausta synergiavaikutuksesta, joka infrastruktuuritoimialoilla on toisiinsa. Esimerkiksi sähköyhtiöön kohdistuva hyökkäys voi sähkönjakeluhäiriöiden lisäksi aiheuttaa häiriöitä jätevesien käsittelylaitoksissa ja vesilaitoksissa, kun näiden laitosten turbiinit ja muut sähkölaitteet pysähtyvät.

Ketjureaktiotkin voivat aiheuttaa suuria vahinkoja ja johtaa laajoihin energiakatkoksiin. Pohjois-Amerikassa ja Euroopassa kahden viime vuoden aikana koetut sähkökatkokset ovat osoittaneet, kuinka haavoittuvia energiainfrastruktuurit ovat ja että on tarpeen kehittää tehokkaita toimenpiteitä merkittävistä toimitushäiriöistä aiheutuvien vaikutusten estämiseksi tai lieventämiseksi. Tällainen tietoverkkoihin kohdistuva terrorismi voi myös pahentaa fyysisen iskun vaikutuksia. Esimerkkinä voidaan mainita perinteinen rakennukseen kohdistuva pommi-isku, jonka seurauksena sähkö- tai puhelinverkko on tilapäisesti poissa käytöstä. Tämä heikentäisi pelastuspalvelujen saatavuutta kunnes sähkö- ja viestintäjärjestelmien varajärjestelmät on saatu käyttöön, ja seurauksena voisi olla kuolonuhrien lisääntyminen ja yleinen paniikki.

3. EUROOPAN KRIITTISET INFRASTRUKTUURIT

3.1. Kriittisen infrastruktuurin määritelmä

Kriittiset infrastruktuurit muodostuvat niistä fyysisistä ja tietoteknisistä laitteista, verkoista, palveluista ja omaisuuseristä, joiden vahingoittaminen tai tuhoaminen vaikuttaisi vakavasti kansalaisten terveyteen, turvallisuuteen ja taloudelliseen hyvinvointiin tai jäsenvaltioiden hallitusten tehokkaaseen toimintaan. Kriittisiä infrastruktuureja on useilla talouden aloilla, esimerkiksi pankki- ja rahoitusala, liikenne ja jakelu, energia, yleishyödylliset laitokset,

terveydenhuolto, elintarvikehuolto, viestintä ja tärkeimmät valtion palvelut. Jotkin kriittiset osatekijät näillä aloilla eivät ole varsinaisesti 'infrastruktuuria', vaan ne ovat verkostoja tai toimitusketjuja, joita käytetään tärkeiden tuotteiden tai palvelujen jakelussa. Esimerkiksi elintarvikkeiden tai veden toimitus kaupunkialueille on riippuvainen eräistä keskeisistä laitteista, mutta myös tuottajien, jalostajien, valmistajien, jakelijoiden ja jälleenmyyjien muodostamasta monimutkaisesta verkostosta.

Kriittisiin infrastruktuureihin kuuluvat seuraavat:

- energialaitokset ja -verkot (esim. sähkön, öljyn ja kaasun tuotantolaitokset, varastointi- ja jalostuslaitokset sekä siirto- ja jakelujärjestelmät)
- viestintä- ja tietotekniikka (esim. televiestintä- ja yleisradiojärjestelmät, tietokoneohjelmistot ja -laitteistot sekä verkot kuten Internet)
- rahoitusala (esim. pankki-, arvopaperi- ja sijoituspalvelut)
- terveydenhuolto (esim. sairaalat, terveydenhuoltolaitokset ja veripalvelu, laboratoriot ja apteekit, etsintä- ja pelastuspalvelut, hätäpalvelut)
- elintarvikkeet (esim. turvallisuus, tuotantovälineet, tukkujakelu ja elintarviketeollisuus)
- vesi (esim. padot, varastointi, käsittely ja verkot)
- liikenne (esim. lentokentät, satamat, intermodaalikalusto, rautatiet, julkisen liikenteen verkot, liikenteenvalvontajärjestelmät)
- vaarallisten aineiden tuotanto, varastointi ja kuljetus (esim. kemialliset, biologiset ja radiologiset aineet sekä ydinaineet)
- julkinen sektori (esim. peruspalvelut, laitokset, tietoverkot, omaisuuserät sekä kansallisesti merkittävät paikat ja muistomerkit).

Näiden infrastruktuurien omistus ja ylläpito voi olla julkisissa tai yksityisissä käsissä. Komissio totesi kuitenkin 10. lokakuuta 2001 antamassaan tiedonannossa 574/2001 seuraavaa: "Jos julkinen valta lujittaa tiettyjä turvatoimia johtuen hyökkäyksistä, jotka on suunnattu koko yhteiskuntaa eikä lentoliikenteessä toimivia vastaan, komissio katsoo, että julkisen vallan on otettava vastatakseen niiden kustannuksista". Sen vuoksi julkisella sektorilla on merkittävä rooli.

Kriittiset infrastruktuurit on määriteltävä niin jäsenvaltioiden tasolla kuin Euroopan tasolla, ja luettelot niistä olisi laadittava vuoden 2005 loppuun mennessä.

Euroopan kriittiset infrastruktuurit liittyvät tiiviisti toisiinsa ja ovat suuressa määrin toisistaan riippuvaisia. Yritysten yhdistyminen, teollisuusalojen rationalisointi, tehokkaat liiketoimintatavat kuten JOT-tuotanto ja väestön keskittyminen kaupunkialueille ovat kaikki vaikuttaneet tähän tilanteeseen. Euroopan kriittiset infrastruktuurit ovat tulleet riippuvaisemmiksi yhteisistä tietotekniikoista kuten Internet, satelliittiradionavigointi ja satelliittiviestintä. Ongelmat voivat johtaa ketjureaktioihin näissä toisistaan riippuvaisissa infrastruktuureissa ja aiheuttaa odottamattomia ja yhä vakavampia häiriöitä tärkeissä

palveluissa. Koska infrastruktuurit liittyvät toisiinsa ja ovat toisistaan riippuvaisia, ne ovat herkempiä häiriöille ja helpommin tuhottavissa.

On tutkittava kriteereitä, joiden perusteella määritetään ne tekijät, jotka tekevät tietystä infrastruktuurista tai infrastruktuurin osasta kriittisen. Näiden valintakriteereiden olisi myös perustuttava alakohtaiseen ja kollektiiviseen asiantuntemukseen. Potentiaalisen kriittisen infrastruktuurin määrittämisessä voitaisiin käyttää kolmea tekijää:

- Laajuus – Kriittisen infrastruktuurin osatekijän menetys luokitellaan kansainväliseksi, valtakunnalliseksi, alueelliseksi tai paikalliseksi sen maantieteellisen alueen laajuuden perusteella, jolla sen menetyksellä tai käytöstä poissaolemisella voisi olla vaikutusta.

- Vakavuus – Vaikutus tai menetys voidaan arvioida olemattomaksi, vähäiseksi, kohtuulliseksi tai suureksi. Potentiaalisen vakavuuden arvioinnissa voitaisiin käyttää muun muassa seuraavia kriteereitä:

    (a) väestöön kohdistuva vaikutus (vaikutusalaan kuuluvan väestön määrä, ihmishenkien menetykset, sairastumiset, vakavat loukkaantumiset, evakuointi);

    (b) taloudelliset vaikutukset (vaikutus BKT:hen, taloudellisten menetysten ja/tai tuotteiden tai palvelujen laadun heikkenemisen suuruus);

    (c) ympäristövaikutukset (vaikutus ympäristöön yleensä ja lähiympäristöön); ja

    (d) keskinäinen riippuvuus (muista kriittisistä infrastruktuuritekijöistä);

    (e) poliittiset vaikutukset (luottamus hallituksen toimintakykyyn).

- Ajallinen näkökohta – Tämän kriteerin avulla osoitetaan, milloin tekijän menetys voisi aiheuttaa vakavan vaikutuksen (välittömästi, 24–48 tunnin kuluessa, viikon kuluttua, jonain muuna ajankohtana).

Monissa tapauksissa psykologiset vaikutukset voivat kuitenkin pahentaa muutoin harmittomia tapahtumia.

Kriittisen infrastruktuurin suojelun nykyistä tilannetta käsitellään teknisessä liitteessä, jossa luodaan alakohtainen katsaus komission tämänhetkisiin saavutuksiin. Katsauksesta ilmenee, että komissiolla on jo paljon kokemusta tältä alalta.

3.2. Turvallisuuden hallinta

Jotta voitaisiin analysoida jäsenvaltioiden kriittisiin infrastruktuureihin kohdistuvia uhkia ja vaaratilanteita sekä niiden haavoittuvuutta ja riippuvuutta toisistaan, on käytettävä useita tietolähteitä. Kaikkien toimialojen ja jäsenvaltioiden on määritettävä EU:n yhdenmukaistetun lähestymistavan mukaisesti kriittisenä pitämänsä infrastruktuuri toimialueellaan sekä turvallisuudesta vastaavat organisaatiot tai henkilöt.

Kaikkia infrastruktuureja ei voida suojella kaikilta uhilta. Esimerkiksi sähkönsiirtoverkot ovat niin suuria, ettei niitä voida aidata tai vartioida. Soveltamalla riskinhallintekniikoita voidaan keskittyä niihin alueisiin, joilla riskit ovat suurimmat, ottaen huomioon uhat, suhteellinen kriittisyys, turvatoimien nykytaso ja käytettävissä olevien liiketoiminnan jatkumisen mahdollistavien strategioiden tehokkuus.

Turvallisuuden hallinta on harkittu prosessi, jossa tunnistetaan riskit ja sekä päätetään toimista että toteutetaan toimia riskin pienentämiseksi määritellylle ja hyväksyttävälle tasolle kustannuksin, jotka voidaan hyväksyä. Tälle lähestymistavalle on ominaista riskien tunnistaminen, mittaaminen ja rajoittaminen määriteltyä tasoa vastaavalle tasolle.

Kriittisen infrastruktuurin suojelu edellyttää jatkuvaa yhteistyötä kriittisen infrastruktuurin omistajien ja ylläpitäjien sekä jäsenvaltioiden viranomaisten välillä. Vastuu riskien hallinnasta fyysisissä laitoksissa, toimitusketjuissa, tietotekniikkajärjestelmissä ja viestintäverkoissa on ensi sijassa omistajilla ja ylläpitäjillä.

Julkisen ja yksityisen sektorin toimijoita on autettava suojelemaan tärkeitä infrastruktuurijärjestelmiä antamalla varoituksia, ohjeita ja tiedotuksia. Ajoittain voi esiintyä erityisiä riskejä tai terrori-iskun uhkia, joihin on reagoitava välittömästi. Tällöin jäsenvaltioiden hallitusten ja alan toimijoiden on koordinoitava toimintansa hyvin. EU:n puolestaan on koordinoitava välttämättömät poliittiset toimet ja sovittava niiden perusteella tarkoista lisäjärjestelyistä asianosaisten kanssa tapauskohtaisesti.

Parhaatkin turvallisuuden hallintaa koskevat suunnitelmat ja niiden täytäntöönpanoa edellyttävät säädökset ovat arvottomia, jollei niitä panna asianmukaisesti täytäntöön. Kokemus on osoittanut, että komission suorittamat riippumattomat turvallisuustarkastukset ovat ainoa tehokas keino varmistaa turvallisuusvaatimusten asianmukainen täytäntöönpano.

4. EDISTYS KRIITTISEN INFRASTRUKTUURIN SUOJELUSSA YHTEISÖN TASOLLA

Euroopan kansalaiset odottavat kriittisten infrastruktuurien toiminnan jatkuvan riippumatta siitä, mitkä organisaatiot ovat niiden yksittäisten osien omistajia tai ylläpitäjiä. Kansalaiset odottavat, että jäsenvaltioiden hallitukset ja EU omaksuvat johtavan rooli tämän varmistamiseksi. He odottavat, että julkisen ja yksityisen sektorin omistajat ja ylläpitäjät kaikilla tasoilla tekevät yhteistyötä sen varmistamiseksi, että Euroopan kansalaisten odottamat palvelut ovat saatavilla.

Kansallisella tasolla toteutettujen toimenpiteiden täydennykseksi Euroopan unioni on jo toteuttanut useita lainsäädännöllisiä toimenpiteitä, joissa vahvistetaan EU:n eri politiikanalojen puitteissa infrastruktuurin suojelun vähimmäisvaatimukset. Erityisesti näin on tapahtunut liikenteen, viestinnän, energian, työterveyden ja -turvallisuuden sekä julkisen terveydenhuollon aloilla. Toimintaa on lisätty Yhdysvalloissa ja Euroopassa tapahtuneiden viimeaikaisten iskujen jälkeen. Tämä johtaa olemassa olevien toimenpiteiden parantamiseen tai laajentamiseen.

EURATOM-sopimuksen puitteissa on vuosikymmenten ajan suoritettu tarkastuksia ydinmateriaalien asianmukaisen käytön valvomiseksi. Säteilysuojelun alalla on paljon lainsäädäntöä, joka koskee radioaktiivisia aineita käsittelevien laitosten toimintaan ja energialähteiden käyttöön liittyviä riskejä.

Kansainvälisen liikenteen alalla Euroopan unioni on antanut lainsäädäntöä, jolla pannaan täytäntöön tai vahvistetaan sopimuksia, joita kansainväliset järjestöt ovat tehneet ilmailun ja meriliikenteen aloilla. Euroopan unioni edistää jatkossakin niiden toimintoja ja osallistuu niihin aktiivisesti kansainvälisellä tasolla. Se kannustaa kolmansia maita, joilla on taloudelliset suhteet EU:hun, panemaan kyseiset sopimukset täytäntöön. Se on tarjonnut apua

joillekin näistä maista, jotta saavutettaisiin yhtenäinen ja pysyvä turvallisuuden taso niin EU:n sisällä kuin sen rajojen ulkopuolellakin.

Yksi edistysaskel on tietoliikenneturvallisuutta käsittelevien virastojen kuten Euroopan verkko- ja tietoturvaviraston (ENISA) perustaminen. Lisäksi lento- ja meriliikenteen turvallisuuden kaltaisilla aloilla on perustettu komission sisäisiä tarkastusyksiköitä, jotka valvovat turvallisuuslainsäädännön täytäntöönpanoa jäsenvaltioissa. Näiden tarkastusten kautta saadaan tarvittavat vertailuarvot, jotka varmistavat yhtenäisen täytäntöönpanon tason unionissa.

Kriittisen infrastruktuurin suojelun nykytilannetta käsitellään teknisesessä liitteessä, jossa luodaan alakohtainen katsaus komission tämänhetkisiin saavutuksiin. Katsauksesta ilmenee, että komissiolla on jo paljon kokemusta tältä alalta.

5. KRIITTISEN INFRASTRUKTUURIN SUOJELUVALMIUDEN PARANTAMINEN EU:SSA

5.1. Euroopan kriittisen infrastruktuurin suojeluohjelma (EPCIP)

Koska potentiaalisia kriittisiä infrastruktuureja on paljon ja niiden ominaispiirteet vaihtelevat, on mahdotonta suojella niitä kaikkia Euroopan tason toimenpiteillä. Toissijaisuusperiaatteen mukaisesti Euroopan unionin on keskityttävä sellaisten infrastruktuurien suojeluun, joilla on valtioiden rajat ylittäviä vaikutuksia, ja jätettävä muut infrastruktuurit jäsenvaltioiden vastuulle, joiden on kuitenkin noudatettava yhteisiä puitteita.

Jo nyt on lukuisia direktiivejä ja asetuksia, joissa säädetään menetelmistä onnettomuuksien havaitsemiseksi, toimintasuunnitelmien laatimisesta yhteistyössä väestönsuojelun kanssa, säännöllisistä harjoituksista ja eri interventiotasojen, julkisten laitosten, keskusorganisaatioiden ja pelastustoimen välisistä selkeistä yhteyksistä. Toisaalta muiden energialaitosten kuin ydinenergialaitosten suojelussa on vielä paljon tehtävää. Kuten teknisesessä liitteessä osoitetaan, kriittisen infrastruktuurin suojelua koskevan yhteisön säännöstön kehitys vaihtelee aloittain.

Useimmilla edellä mainituista aloista työt ovat käynnissä ja jäsenvaltioiden asiantuntijoiden ja kyseessä olevien toimialojen kanssa tehdään yhteistyötä mahdollisten puutteiden havaitsemiseksi ja (oikeudellisten tai muiden) korjaustoimenpiteiden toteuttamiseksi. Lukuisia verkostoja ja turvakomiteoita on perustettu.

Komissio raportoi muille toimielimille edistyksestä vuosittain erityisessä tiedonannossa. Se analysoi kunkin toimialan osalta yhteisön tekemän työn edistymistä riskien arvioinnin ja suojelukeinojen kehittämisen alalla tai meneillä olevia/suunniteltuja oikeudellisia toimia saadakseen niiltä kannanottoja. Komissio ottaa lisäksi tässä tiedonannossa tarvittaessa esille parannuksia ja horisontaalisia järjestelytoimenpiteitä, jotka edellyttävät yhdenmukaistamista, yhteensovittamista ja yhteistyötä. Tämä tiedonanto, johon yhdistetään kaikkia aloja koskevat analyysit ja toimenpiteet, muodostaa perustan Euroopan kriittisen infrastruktuurin suojeluohjelmalle (European Programme for Critical Infrastructure Protection – EPCIP).

Tämän ohjelman tarkoituksena on tukea alan toimijoita ja jäsenvaltioiden hallituksia kaikilla tasoilla EU:ssa yksittäiset tehtävä- ja vastuualueet huomioon ottaen. Komissio katsoo, että EU:n jäsenvaltioiden kriittisen infrastruktuurin suojelun asiantuntijoista muodostuva verkosto voisi auttaa komissiota ohjelman laatimisessa – tämä kriittisen infrastruktuurin

varoitusverkosto (Critical Infrastructure Warning Information Network – CIWIN) olisi perustettava mahdollisimman pian vuonna 2005.

Verkoston perustamisen odotetaan ennen kaikkea edistävän tietojenvaihtoa yhteisistä uhista ja heikkouksista sekä asianmukaisista toimenpiteistä ja strategioista riskin pienentämiseksi kriittisen infrastruktuurin suojelun tukemiseksi. Jäsenvaltioiden olisi sen vuoksi varmistettava, että merkitykselliset tiedot toimitetaan kaikille asianmukaisille valtion laitoksille ja virastoille, pelastusorganisaatiot mukaan luettuina, ja asiaankuuluville toimialajärjestöille, jotka puolestaan huolehtivat tiedotuksesta kriittisen infrastruktuurin omistajille ja ylläpitäjille jäsenvaltioiden välisen yhteysverkoston kautta.

EPCIP muodostaisi pysyvän foorumin, jossa kilpailun, vastuuvelvollisuuden ja tietojen luottamuksellisuuden asettamat rajoitukset voidaan tasapainottaa turvallisemman kriittisen infrastruktuurin tuomien etujen kanssa. Alan toimijat ovat tässä prosessissa tiiviisti mukana. Sen avulla on mahdollista toimittaa enemmän tietoja kumppaneille erityisistä uhkatilanteista, jolloin ne pystyvät toteuttamaan toimenpiteitä mahdollisiin seurauksiin varautumiseksi. Omistajien ja ylläpitäjien vastuu tehdä itse omaisuutensa suojelua koskevat päätökset ja suunnitelmat säilyy ennallaan.

Silloin kun alakohtaisia standardeja ei ole tai kun kansainvälisiä normeja ei vielä ole vahvistettu, Euroopan standardointikomitea (CEN) ja muut asianmukaiset standardointiorganisaatiot voisivat avustaa verkostoa ja ehdottaa yhtenäisiä alakohtaisia ja mukautettuja turvallisuusstandardeja kaikille asianomaisille aloille. Tällaisia standardeja olisi ehdotettava myös kansainvälisellä tasolla ISO:n kautta tasavertaisten toimintaedellytysten luomiseksi.

Kun puhutaan kriittiseen infrastruktuuriin kohdistuvista kansallisista uhista, terrorismi mukaan luettuna, on noudatettava tiettyä varovaisuutta, jotta ei turhaan huolestuteta EU:n kansalaisia tai mahdollisia matkailijoita ja sijoittajia. Terrorismi on jatkuva uhka, mutta politiikantekijöiden tehtävänä on rohkaista kaikkia jatkamaan elämäänsä mahdollisimman normaalisti. On myös pyrittävä kunnioittamaan yksityisyyden suojaa sekä unionin sisällä että sen ulkopuolella. Kuluttajien ja toiminnanharjoittajien on voitava luottaa siihen, että tietoja käsitellään oikein, luottamuksellisesti ja luotettavasti. On oltava järjestelmä sen varmistamiseksi, että luottamuksellisia tietoja käsitellään asianmukaisesti ja suojellaan luvattomalta käytöltä tai paljastamiselta.

Suuri osa sekä EU:n että jäsenvaltioiden kriittisistä infrastruktuureista ylittää EU:n rajat. On koko maanosan ylittäviä putkistoja, tietotekniikkapalveluille välttämättömiä kaapeleita kulkee syvällä merenpohjassa jne. Tämä merkitsee sitä, että kansainvälinen yhteistyö on tärkeää luotaessa pysyviä, dynaamisia kansallisia ja kansainvälisiä kumppanuuksia kriittisen infrastruktuurin omistajien/ylläpitäjien ja kolmansien maiden hallitusten välille, erityisesti silloin kun on kyse maista, jotka toimittavat suoraan energiatuotteita unioniin.

5.2. Kriittisen infrastruktuurin suojeluohjelman (EPCIP) täytäntöönpano

Kriittisen infrastruktuurin suojelu edellyttää infrastruktuurin omistajien ja ylläpitäjien, sääntelyviranomaisten, ammatillisten ja toimialajärjestöjen sekä jäsenvaltioiden ja komission aktiivista osallistumista. Niiden tietojen perusteella, joita on saatu jäsenvaltioilta ja verkoston kautta, Euroopan kriittisen infrastruktuurin suojeluohjelman tavoitteena on kriittisten infrastruktuurien määrittäminen, niiden haavoittuvuuden ja keskinäisen riippuvuuden analysointi ja ratkaisujen kehittäminen uhilta suojautumista ja niihin varautumista varten. Tähän sisältyisi toimialojen auttaminen ymmärtämään uhat ja niiden

seuraukset riskinarvioinneissaan. Jäsenvaltioiden lainvalvontaviranomaisten ja väestönsuojeluviranomaisten olisi varmistettava, että EPCIP on olennainen osa niiden suunnittelu- ja valistustoimintaa.

Komission yksiköt kehittävät koordinoidusti verkoston kanssa muita lainsäädännön antamisen ja/tai tiedonvälityksen muodossa toteutettavia toimia. Poliisipäälliköiden toimintaryhmällä ja Europolilla on merkittävä rooli turvallisuustasoja koskevien tietojen ja tiedustelutietojen välittämisessä jäsenvaltioiden lainvalvontaviranomaisille, joiden puolestaan on pidettävä yhteyttä kriittisen infrastruktuurin omistajiin ja ylläpitäjiin ja annettava niille tietoja uhkista sekä avustettava niitä turvaohjeiden antamisessa ja terrorismin vastaisten turvallisuusstrategioiden kehittämisessä.

Jäsenvaltioiden hallitukset pitävät edelleen toiminnassa ja/tai kehittävät tietokantoja kansallisesti merkittävästä kriittisestä infrastruktuurista. Ne ovat myös vastuussa asianmukaisten suunnitelmien kehittämisestä, validoinnista ja tarkastamisesta palvelujen jatkuvuuden varmistamiseksi alueellaan. EPCIP-ohjelmaa laadittaessa komissio tekee ehdotuksia tällaisten tietokantojen vähimmäissisällöstä ja muodosta sekä siitä, kuinka ne olisi liitettävä toisiinsa.

Jäsenvaltioiden hallitukset puolestaan jatkavat merkityksellisten tiedustelutietojen ja varoitusten välittämistä kriittisen infrastruktuurin omistajille ja ylläpitäjille (ja tarvittaessa muille jäsenvaltioille) sekä tiedottamista kussakin uhka-/varoitusluokassa sovitusta toimintatavasta.

Kriittisen infrastruktuurin omistajat ja ylläpitäjät turvaavat omaisuutensa riittävällä tavalla panemalla turvallisuussuunnitelmansa aktiivisesti täytäntöön ja järjestämällä säännöllisesti tarkastuksia ja harjoituksia sekä tekemällä arviointeja ja suunnitelmia. Jäsenvaltioiden tehtävänä on valvoa prosessia kokonaisuudessaan, kun taas komission on varmistettava yhdenmukainen täytäntöönpano kaikkialla unionissa asianmukaisten tarkastusjärjestelmien avulla.

5.3. Kriittisen infrastruktuurin suojeluohjelman tavoitteet ja edistymistä ilmaisevat indikaattorit

Kriittisen infrastruktuurin suojeluohjelman (EPCIP) tavoitteena ja komission velvollisuutena on varmistaa, että kriittisen infrastruktuurin suojelu on riittävällä ja yhtenäisellä tasolla kaikkialla unionissa, että haavoittuvia kohtia on mahdollisimman vähän ja että on olemassa nopeat ja testatut järjestelyt tilanteen palauttamiseksi entiselleen. EPCIP-ohjelmaa kehitetään jatkuvasti ja yhteisössä esiintyvien ongelmien ja huolenaiheiden tasalla pysyminen edellyttää säännöllisiä tarkastuksia.

Onnistumista mitataan seuraavien tekijöiden perusteella:

- jäsenvaltioiden hallitusten EPCIP-ohjelmassa asetettujen prioriteettien mukaisesti määrittämät ja luetteloimat kriittiset infrastruktuurit, jotka kuuluvat niiden toimivallan piiriin;

- yritysten toimialallaan ja hallituksen kanssa harjoittama yhteistyö tietojen jakamiseksi ja sellaisten vaaratilanteiden todennäköisyyden pienentämiseksi, joista aiheutuisi laajalle ulottuvia tai pitkäaikaisia kriittisen infrastruktuurin häiriöitä;

- Euroopan yhteisö laatii yhteisen menetelmän kriittisen infrastruktuurin turvallisuuden takaamiseksi kaikkien julkisten ja yksityisten toimijoiden yhteistyöllä.

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.