AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA

Brüsszel, 20.10.2004
COM(2004) 702 végleges

A BIZOTTSÁG KÖZLEMÉNYE A TANÁCS ÉS AZ EURÓPAI PARLAMENT RÉSZÉRE

A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben

TARTALOMJEGYZÉK

1. BEVEZETŐ 3

2. VESZÉLY 3

3. EURÓPA LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁI 3

3.1. Mi tartozik a létfontosságú infrastruktúrák körébe? 3

3.2. A biztonsággal kapcsolatos irányítás 5

4. A LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK VÉDELMÉVEL KAPCSOLATBAN KÖZÖSSÉGI SZINTEN EDDIG ELÉRT EREDMÉNYEK 6

5. AZ EU LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK VÉDELMÉRE VONATKOZÓ KÉPESSÉGE 7

5.1. A létfontosságú infrastruktúrák védelmére vonatkozó európai program 7

5.2. Az EPCIP végrehajtása 9

5.3. Az EPCIP célkitűzései és eredménymutatói 10

TECHNIKAI MELLÉKLET 11

1. BEVEZETŐ

Az Európai Tanács 2004. júniusi ülése felkérte a Bizottságot és a főképviselőt, hogy készítsenek egy átfogó stratégiát a létfontosságú infrastruktúrák védelmére.

E közlemény áttekinti a Bizottság létfontosságú infrastruktúrák védelmével kapcsolatos jelenlegi intézkedéseit, és további intézkedéseket javasol a meglévő eszközök megerősítése és az Európai Tanácstól kapott megbízások teljesítése céljából.

2. VESZÉLY

A létfontosságú infrastruktúrákat fenyegető katasztrofális terrortámadások lehetősége egyre nő. A létfontosságú infrastruktúrák ipari ellenőrző rendszerei elleni támadás következményei rendkívül eltérőek lehetnek. Általánosan elfogadott, hogy egy sikeres kibertámadás legrosszabb esetben is csupán kevés sérüléssel járna, de a létfontosságú infrastrukturális szolgáltatások szempontjából veszteséget eredményezhet. Például a nyilvános telefonkapcsolási hálózat elleni sikeres kibertámadás miatt az ügyfelek nélkülöznék a telefonszolgáltatást mindaddig, míg a szakemberek elvégzik a kapcsolási hálózat helyreállítását és javítását. A vegyi vagy folyékony földgázt előállító üzemek ellenőrző rendszerei elleni támadás sokkal több életet követelhet, és jelentős fizikai kárt okozhat.

Az infrastruktúrák katasztrofális meghibásodásának másik típusa az lehet, amikor az infrastruktúra egy részének meghibásodása a többi meghibásodásához vezet, ami dominóhatást válthat ki. Ilyen meghibásodás az infrastrukturális ágazatok egymásra gyakorolt szinergetikus hatása következtében alakulhat ki. Ennek egy egyszerű példája lehet a villamosáram-szolgáltató közüzemek elleni támadás, ahol megszakad a villamosáram-elosztás; a szennyvízkezelő telepeken és a vízműveknél szintén meghibásodás történik, mivel a létesítmények turbinái és más elektromos készülékei leállhatnak.

Az egymást követő események láncolata szintén nagy károkat okozhat, a közüzemek általános leállását idézheti elő. Az elmúlt két évben az Észak-Amerikában és Európában bekövetkezett áramszünetek nyilvánvalóvá tették az energiaipari infrastruktúrák sebezhetőségét és annak szükségességét is, hogy a fontos ellátások megszakadásának következményei megelőzésére vagy mérséklésére hatékony intézkedéseket kell találni. A kiberterrorizmus alkalmazása a fizikai támadások hatását is felerősítheti. Jó példa lehet erre egy bizonyos épület elleni hagyományos bombatámadás, amely a villamosáram- és telefonszolgáltatás ideiglenes megszakításával jár együtt. Ennek következtében veszélyhelyzetben – a tartalék villamosáram-szolgáltató vagy tájékoztató rendszerek újraműködtetéséig és használatáig – alacsonyabb hatásfokú válaszlépések megtételére kerülhet sor, ami növelheti a sérültek számát és az általános pánikot.

3. EURÓPA LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁI

3.1. Mi tartozik a létfontosságú infrastruktúrák körébe?

A létfontosságú infrastruktúrákhoz azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági

jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából. A létfontosságú infrastruktúrák több gazdasági ágazatra kiterjednek, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány létfontosságú eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják. Például a jelentős városi térségek élelmiszer- vagy vízellátása néhány kulcsfontosságú létesítménytől függ, ugyanakkor a termelők, feldolgozók, gyártók, forgalmazók és kiskereskedők összetett hálózata is szükséges az ellátás biztosításához.

A létfontosságú infrastruktúrák körébe a következők tartoznak:

- energiaipari létesítmények és hálózatok (pl. villamosenergia-, kőolaj- és földgáztermelés, tárolók és finomítók, szállító- és elosztóhálózat).

- tájékoztatás és információs technológia (pl. távközlés, műsorszolgáltató rendszerek, szoftver, hardver és hálózatok, az Internet is)

- pénzügyek (pl. bankügyletek, értékpapír és befektetés)

- egészségügy (pl. kórházak, egészségügyi és vérellátó létesítmények, laboratóriumok és gyógyszerellátók, felkutatás és mentés, sürgősségi ellátás)

- élelmiszer (pl. biztonság, termelési eszközök, nagykereskedelmi forgalmazás és élelmiszeripar)

- vízellátás (pl. gátak, víztárolás, -kezelés és -hálózatok)

- közlekedés (pl. repülőterek, kikötők, intermodális létesítmények, vasúti és anyagszállítási hálózatok, forgalomirányító rendszerek)

- veszélyes anyagok előállítása, tárolása és szállítása (pl. vegyi, biológiai, radioaktív és nukleáris anyagok)

- állami infrastruktúrák (pl. létfontosságú szolgáltatások, berendezések, információs hálózatok, eszközök és jelentős nemzeti helyek és műemlékek)

Ezek az infrastruktúrák részben az állam, részben a magánszféra tulajdonában vannak, illetve azokat az állam vagy a magánszféra működteti. A Bizottság azonban a 2001. október 10-i 574/2001 közleményében kijelentette: „A társadalom egésze – és nemcsak az ipari szereplők – ellen irányuló támadások következtében az állami hatóságok bizonyos biztonsági intézkedéseinek fokozását az államnak kell biztosítania". Ezért lényeges szerepet tölt be a közszféra.

A létfontosságú infrastruktúrákat tagállami és európai szinten is meg kell határozni, és az ilyen infrastruktúrák jegyzékét 2005 végéig össze kell állítani.

Európa létfontosságú infrastruktúrái nagymértékben összekapcsolódnak és egymástól függnek. A vállalategyesítés, az ipari racionalizáció, a hatékony üzleti gyakorlatok, például az éppen időben történő gyártás, valamint a népesség városi térségekbe történő tömörülése mind

hozzájárult e helyzet kialakulásához. Európa létfontosságú infrastruktúrái esetében egyre inkább szükség van a közös információs technológiák – például az internet és az űrben telepített rádiónavigáció és hírközlés – alkalmazására. A problémák végigvonulhatnak az egymással összefüggő infrastruktúrákon, az alapvető szolgáltatások váratlan és egyre komolyabb meghibásodását okozhatják. Az összekapcsolódás és az interdependencia miatt ezek az infrastruktúrák kiszolgáltatottabbak az összeomlás vagy megsemmisítés szempontjából.

Tanulmányozni kell azon tényezők meghatározására szolgáló kritériumokat, amelyek miatt egy bizonyos infrastruktúra vagy az infrastruktúra egy bizonyos eleme létfontosságúnak tekinthető. Az említett kiválasztási kritériumok megállapításánál ágazati és közös szakismereteket is fel kell használni. A létfontosságú infrastruktúrák meghatározásához három tényező alkalmazása ajánlott:

- Hatókör – a létfontosságú infrastruktúra valamely elemével kapcsolatos veszteséget azon földrajzi terület nagysága alapján számítják ki, amelyet a veszteség vagy az adott szolgáltatás megszűnése érinthet - nemzetközi, nemzeti, tartományi/területi vagy helyi.

- Nagyságrend – a hatás mértékét a következőképpen lehet értékelni: nincs hatás, minimális, mérsékelt vagy jelentős. Többek között a következő szempontok alkalmazhatók a nagyságrend megállapításához:

    (a) A lakossággal kapcsolatos hatás (az érintett lakosság száma, áldozatok, betegségek, komoly sérülés, evakuálás);

    (b) Gazdasági (GDP-hatás, a gazdasági veszteség jelentősége és/vagy a termékek vagy szolgáltatások színvonalának fokozatos romlása);

    (c) Környezetvédelmi (a lakosságra és a környezetére gyakorolt hatás); és

    (d) Interdependencia (a létfontosságú infrastruktúrák egyéb elemei között);

    (e) Politikai (az állam iránti bizalom);

- Időbeli hatás – e szempont annak megállapítására szolgál, hogy egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejthet ki komoly hatást (pl. azonnali, 24–48 óra, egy hét, egyéb).

Sok esetben azonban a pszichológiai hatások egyébként kisebb jelentőségű következményekkel is járhatnak.

A létfontosságú infrastruktúrák védelmével kapcsolatos legfrissebb fejleményeket az technikai melléklet tartalmazza, amely ágazatonként tekinti át a Bizottság által eddig elért eredményeket. Ezek azt bizonyítják, hogy a Bizottság jelentős tapasztalatot szerzett e területen.

3.2. A biztonsággal kapcsolatos irányítás

A tagállamok létfontosságú infrastruktúrái elemeivel, valamint azok egymástól való függőségével kapcsolatos, a veszélyekre, váratlan eseményekre és a sebezhetőségre vonatkozó elemzés elvégzéséhez több forrásból származó információra van szükség. Minden ágazatnak és tagállamnak az EU harmonizált szabálya szerint a saját hatáskörén belül és a

biztonságért felelős szervezetek vagy személyek segítségével kell meghatároznia a létfontosságú infrastruktúrákat.

Nem lehet minden infrastruktúrát minden veszéllyel szemben megvédeni. Például a villamosáram-továbbító hálózatok túlságosan nagy kiterjedésűek ahhoz, hogy őrzésüket vagy védelmüket biztosítani lehessen. A kockázatkezelési technikák alkalmazásával a legnagyobb veszélynek kitett térségekre lehet irányítani a figyelmet, tekintetbe véve a veszélyt, a relatív fontosságot, a biztonságvédelem adott szintjét és a folyamatos működés érdekében alkalmazható, a hatások mérséklésére vonatkozó stratégiák hatékonyságát.

A biztonsággal kapcsolatos irányítás tudatos folyamat, amely a kockázat megállapítását, valamint az adott kockázat meghatározott – elfogadható költségek mellett elfogadható – szintre való csökkentésére irányuló intézkedések meghozatalát és végrehajtását foglalja magában. E módszerre a kockázatoknak a kijelölt szintnek megfelelő megállapítása, mérése és ellenőrzése jellemző.

A létfontosságú infrastruktúrák védelméhez (CIP) a létfontosságú infrastruktúrák tulajdonosai és üzemeltetői, valamint a tagállami hatóságok közötti következetes, együttműködő partnerség szükséges. A fizikai létesítményekkel, ellátási láncokkal, információs technológiákkal és hírközlő hálózatokkal kapcsolatos kockázatkezelés elsősorban a tulajdonosok és az üzemeltetők feladata.

Figyelmeztetések, tanácsadói vélemények és tájékoztatók kiadásával kell segíteni a köz- és magánszféra érintett szereplőit a kulcsfontosságú infrastrukturális rendszerek védelmének biztosításában. Időről időre terrortámadások konkrét kockázata vagy veszélye fenyegethet, ami azonnali válaszlépést igényel. Ilyen estekben a tagállamok kormányai és az iparág részéről jól összehangolt, koncentrált műveleti válaszlépésekre van szükség. Ilyen körülmények között az EU-nak kell összehangolnia a szükséges politikai válaszlépéseket, és ennek alapján eseti alapon kerül sor az érintettekkel való, a részletes támogató intézkedésekre vonatkozó megállapodásra.

A biztonsággal kapcsolatos irányításra vonatkozó legkiválóbb tervek és az alkalmazásukat kikényszerítő jogszabályok sem érnek semmit a megfelelő végrehajtás nélkül. A tapasztalatok azt bizonyítják, hogy a biztonsági követelmények megfelelő végrehajtásának biztosítására a végrehajtás független bizottsági biztonsági ellenőrzése az egyedüli hatékony eszköz.

4. A LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK VÉDELMÉVEL KAPCSOLATBAN KÖZÖSSÉGI SZINTEN EDDIG ELÉRT EREDMÉNYEK

Az európaiak remélik, hogy a létfontosságú infrastruktúrák továbbra is működni fognak függetlenül attól, hogy mely szervezetek birtokolják vagy működtetik az alkotóelemeit. Azt várják, hogy a tagállamok kormányai és az EU vezető szerepet játszanak annak biztosításában, hogy ez így is történik. Elvárják, hogy valamennyi kormányzati szint és a magánszférabeli tulajdonosok és üzemeltetők működjenek együtt az európaiak számára létfontosságú szolgáltatások folyamatosságának biztosítása érdekében.

A nemzeti szinten megtett intézkedések kiegészítéseként az Európai Unió már számos jogszabályi intézkedést hozott, amelyek a különböző EU-politikák keretében határozzák meg az infrastruktúra védelmére vonatkozó minimumkövetelményeket. Különösen így van ez a közlekedési, hírközlési, energia-, foglalkozás-egészségügyi és biztonsági, valamint a

közegészségügyi ágazatban. A legutóbbi, Amerika és Európa elleni támadásokat követően fokozódtak az intézkedések. Ezek a meglévő intézkedések továbbfejlesztését vagy kiterjesztését eredményezik majd.

A vizsgálatokat évtizedekig az EURATOM-Szerződés keretében hajtották végre a nukleáris anyagok megfelelő alkalmazásának ellenőrzése céljából. A sugárvédelem terén számos olyan jogszabály létezik, amely a létesítmények működésével és a radioaktív anyagokat tartalmazó források alkalmazásával kapcsolatos veszélyekre vonatkozik.

Az Európai Unió a nemzetközi közlekedés terén olyan jogszabályokat fogadott el, amelyek a legfőbb nemzetközi repülési és tengerészeti szervezetek által kötött megállapodásokat hajtják végre vagy alkalmazzák. Az említett szervezetek nemzetközi tevékenysége tekintetében az Európai Unió továbbra is támogatást nyújt és aktív szerepet vállal. Arra ösztönzi az EU-val gazdasági kapcsolatban álló harmadik országokat, hogy alkalmazzák az említett megállapodásokat. Az EU bizonyos harmadik országoknak támogatást nyújtott azzal a céllal, hogy az EU határain belül és kívül a biztonság homogén és állandó szintjét érje el.

Újabb lépésként ügynökségek jöttek létre, például a tájékoztatás biztonsága terén az Európai Hálózat- és Információvédelmi Ügynökség. Ezenkívül például a repülés- és a tengeri biztonság terén felügyeleti szolgálatok jöttek létre a Bizottságon belül annak ellenőrzésére, hogy a tagállamok végrehajtják-e a biztonságra vonatkozó jogszabályokat. Ezek az ellenőrzések adják a szükséges viszonyítási alapot, amely azonos végrehajtási szintet biztosít az Unión belül.

A létfontosságú infrastruktúrák védelmével kapcsolatos legfrissebb fejleményeket az technikai melléklet tartalmazza, amely ágazatonként tekinti át a Bizottság által eddig elért eredményeket. Ezek azt bizonyítják, hogy a Bizottság jelentős tapasztalatot szerzett e területen.

5. AZ EU LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK VÉDELMÉRE VONATKOZÓ KÉPESSÉGE

5.1. A létfontosságú infrastruktúrák védelmére vonatkozó európai program

A létfontosságú infrastruktúrák nagy száma és a sajátosságaik miatt lehetetlen mindegyik védelmét európai szintű intézkedéssel biztosítani. A szubszidiaritás elvének alkalmazásával Európának az országhatárokon átterjedő hatással rendelkező infrastruktúrák védelmére kell a az erejét összpontosítania, míg a többi esetében a védelem a tagállamok kizárólagos feladata, de közös keretekben.

Számos irányelv és rendelet már létrejött, amelyek megszabják a balesetek felderítésének, a beavatkozással kapcsolatos tervek polgári védelemmel együttműködésben történő kialakításának, a különböző beavatkozási szintek – a közellátást biztosító művek, központi szervezetek és sürgősségi szolgálatok – közötti rendszeres gyakorlatok és egyértelmű kapcsolatok létrehozásának módját. Másrészt még sok a teendő a nem nukleáris energiaipari létesítmények védelme terén. Az technikai mellékletben bemutatottak szerint a létfontosságú infrastruktúrák védelme terén a közösségi vívmányok eltérő fejlettségi szinten állnak.

A fent említett területek nagy részén folyamatos a munka, és kialakult az együttműködés a tagállamok szakértőivel és az érintett gazdasági ágazatokkal az esetleges hiányosságok és az

alkalmazandó korrekciós intézkedések (jogi vagy egyéb) megállapítása céljából. Több hálózat és biztonsági bizottság jött létre.

A Bizottság minden naptári évben közleményben számol be az elért eredményekről a többi intézménynek. Ágazatonként elemzi a közösségi tevékenység fejleményeit a kockázatfelmérés, a védelmi technikák kidolgozása terén, illetve a folyamatban lévő/tervezett jogi intézkedéseket a javaslataik összegyűjtése céljából. A Bizottság továbbá, amennyiben szükséges, e közleményben frissítéseket és horizontális szervezeti intézkedéseket fog javasolni, amelyek szükségesek a harmonizációhoz, az összhanghoz vagy az együttműködéshez. E közlemény, amely egyesíti az összes ágazati elemzést és intézkedést, képezi a létfontosságú infrastruktúrák védelmére vonatkozó európai program (EPCIP) alapját.

Az említett program célja, hogy támogassa az iparágat és a tagállamok kormányait az EU valamennyi szintjén, tekintetbe véve egyéni feladataikat és felelősségi körüket. A Bizottságnak az a véleménye, hogy az EU-tagállamok CIP-szakértőit összegyűjtő hálózat segítséget nyújthatna a Bizottságnak a program kidolgozásában – a létfontosságú infrastruktúrákkal kapcsolatos figyelmeztető információs hálózatot (CIWIN) 2005-ben a lehető leghamarabb létre kell hozni.

A hálózat létrehozása elsősorban a közös veszélyekkel és sebezhető pontokkal kapcsolatos információk, valamint a létfontosságú infrastruktúrák védelmével kapcsolatos kockázat csökkentésére irányuló megfelelő intézkedések és stratégiák cseréjének ösztönzésében nyújthat segítséget. A tagállamok pedig így biztosíthatnák, hogy az adott információ eljut valamennyi illetékes állami részleghez és hivatalhoz, beleértve a sürgősségi szolgáltatást nyújtó szervezeteket, amelyek tájékoztatják az érintett ágazat szervezeteit, hogy azok pedig a tagállamokon belül létrehozott kapcsolathálózaton keresztül tájékoztassák a létfontosságú infrastruktúra érintett tulajdonosait és működtetőit.

Az EPCIP támogatná egy folyamatos fórum kialakítását, ahol a versenykorlátokat, a felelősséget és az információk érzékenységét a létfontosságú infrastruktúrák nagyobb biztonságának előnyei ellensúlyoznák. E folyamat során közvetlen konzultációkat folytatnak az iparággal. Az iparág elősegíti, hogy a partnerek több információt kapjanak az adott veszélyhelyzetekről, ami lehetővé teszi, hogy intézkedéseket tegyenek a következmények kezelésére. A tulajdonosok és az üzemeltetők feladata és felelőssége, hogy az eszközeik védelmére vonatkozó döntéseik és terveik ne változzanak.

Ha nem léteznek ágazati előírások, vagy még nem jöttek létre nemzetközi normák, az Európai Szabványügyi Bizottság (CEN) és az egyéb szabványügyi szervezetek támogathatják a hálózatot, valamint egységes ágazati biztonsági és az összes érintett ágazathoz igazított szabványokat javasolhatnak. Az ilyen szabványokat nemzetközi szinten, az ISO-n keresztül is elő kell terjeszteni annak érdekében, hogy e tekintetben egyenlő feltételek jöjjenek létre.

A létfontosságú infrastruktúrákat fenyegető nemzetbiztonsági veszélyekre – többek között a terrorizmusra – való hivatkozáskor figyelmet kell fordítani arra, hogy elkerüljék az indokolatlan aggodalmakat az EU-n belül, valamint a turisták és a befektetők körében. A terrorizmus állandó fenyegetést jelent, de a politikaformálók feladata, hogy mindenkit arra buzdítsanak, hogy a lehetőségek szerint zavartalanul folytassák életüket. A magánélet tiszteletben tartásához való jogot is figyelembe kell venni az Unión belül és kívül is. Az ügyfeleknek és az üzemeltetőknek bizonyosnak kell lenniük abban, hogy az információkat gondosan, bizalmasan és megbízhatóan kezelik. Szükség van egy megfelelő keretre annak

biztosításához, hogy a minősített ismereteket megfelelően kezelik és védik a jogosulatlan használattal vagy nyilvánosságra hozatallal szemben.

Mind az EU, mind a tagállamok létfontosságú infrastruktúráinak nagy része átnyúlik az EU határain. A csővezetékek földrészeket hálóznak be, az információs technológiához feltétlenül szükséges kábeleket mélyen a tengerfenéken fektetik le stb. Ez azt jelenti, hogy a nemzetközi együttműködés fontos eleme a létfontosságú infrastruktúrák tulajdonosai/üzemeltetői és a harmadik országok kormányai, különösen az Unió közvetlen energiaellátói közötti folyamatos, dinamikus, nemzeti és nemzetközi partnerség kialakításának.

5.2. Az EPCIP végrehajtása

A létfontosságú infrastruktúrák védelméhez az infrastruktúrák tulajdonosainak és működtetőinek, a szabályozók, szakmai szervezetek és ágazati szövetségek, valamint a tagállamok és a Bizottság aktív részvétele szükséges. A tagállamok interfészei és a hálózat által nyújtott információk alapján az EPCIP célkitűzései a következők: a létfontosságú infrastruktúrák meghatározásának folytatása, a sebezhető pontok és az interdependencia elemzése, valamint megoldások indítványozása valamennyi veszéllyel kapcsolatos védelem és felkészülés tekintetében. Ennek része lenne, hogy kockázatfelméréseik elkészítésben a veszélyek és következmények felismerésével támogatják az ipari ágazatokat. A tagállamok bűnüldöző szerveinek és a polgárvédelmi mechanizmusnak biztosítaniuk kell, hogy tervezésüknek és a tájékoztatás növelésének az EPCIP szerves része.

A bizottsági szolgálatok a hálózattal szoros összhangban további intézkedéseket dolgoznak majd ki, amelyeknek a jogszabályok elfogadásából és/vagy az információterjesztésből kell állniuk. A rendőrfőnökök munkacsoportjának és az Europolnak szerepet kellene játszania az adott biztonsági szintről és a hírszerzéstől származó információk tagállami bűnüldözési szervezetekhez való eljuttatásában, amelyek pedig érintkezésbe lépnének a létfontosságú infrastruktúrák tulajdonosaival és üzemeltetőivel és tájékoztatnák őket az adott veszélyre vonatkozó információkról, segítséget nyújtanának a biztonságvédelmi tanácsadásban és a terrorizmus elleni küzdelemre vonatkozó biztonságvédelmi stratégiák kialakításában.

A tagállamok kormányai megtartják és/vagy kialakítják és fenntartják a nemzeti szempontból létfontosságú infrastruktúrák adatbázisait, valamint felelősek a vonatkozó tervek kialakításáért, jóváhagyásáért és ellenőrzésért, így biztosítják a hatáskörükbe tartozó szolgáltatások folyamatosságát. Az EPCIP megállapításakor a Bizottság javaslatokat tesz az ilyen adatbázisok minimális tartalmára és formájára, valamint az összekapcsolásuk módjára vonatkozóan.

A tagállamok kormányai pedig folytatják a létfontosságú infrastruktúrák tulajdonosainak és üzemeltetőinek (valamint adott esetben a többi tagállam) tájékoztatását az aktuális értesülésekről és figyelmeztetésekről, valamint a veszély/az érintettek figyelmeztetése szintjének megfelelő válaszlépésről.

A létfontosságú infrastruktúrák tulajdonosai és üzemeltetői a biztonsági terveik tényleges megvalósítása, valamint rendszeres ellenőrzések, gyakorlatok, felmérések és tervek végrehajtása révén biztosítanák eszközeik megfelelő biztonságát. A tagállamoknak ellenőrizniük kell az egész folyamatot, míg a Bizottságnak megfelelő felügyeleti rendszerek segítségével egységes végrehajtást kell biztosítania Unió-szerte.

5.3. Az EPCIP célkitűzései és eredménymutatói

Az EPCIP célja és a Bizottság feladata annak biztosítása lenne, hogy a létfontosságú infrastruktúrák biztonságvédelmének megfelelő és egységes szintje, minimális hibaelkövetés és gyors, ellenőrzött helyreállító rendelkezések garantáltak legyenek Unió-szerte. Az EPCIP egy állandó folyamat lenne és rendszeres felülvizsgálat szükséges ahhoz, hogy folyamatosan értesüljünk a Közösségen belüli problémákról és aggodalmakról.

A siker a következőkkel mérhető:

- A létfontosságú infrastruktúrák nyilvántartásának a tagállamok kormányai által a hatáskörükön belül az EPCIP prioritásai szerint történő meghatározása és létrehozása;

- Az információcsere, valamint a létfontosságú infrastruktúrák kiterjedt vagy hosszú ideig tartó összeomlását okozó váratlan események valószínűségének csökkentése érdekében az ágazatokon belül és a kormányzattal együttműködő vállalatok;

- Az Európai Közösség elhatározza, hogy valamennyi köz- és magánszereplő együttműködésével közös módszert alakít ki a létfontosságú infrastruktúrák biztonságának megoldására.

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.