KOMISIA EURÓPSKYCH SPOLOČENSTIEV

Brusel, 20.10.2004
KOM(2004) 702 v konečnom znení

OZNÁMENIE KOMISIE
RADE A EURÓPSKEMU PARLAMENTU

Ochrana najdôležitejšej infraštruktúry v boji proti terorizmu

OBSAH

1. ÚVOD 3

2. HROZBA 3

3. NAJDÔLEŽITEJŠIE INFRAŠTRUKTÚRY EURÓPY 3

3.1. Čo je najdôležitejšia infraštruktúra 3

3.2. Riadenie bezpečnosti 5

4. POKROK DOSIAHNUTÝ V OCHRANE NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY NA ÚROVNI SPOLOČENSTVA 6

5. ZVÝŠENIE VÝKONNOSTI OCHRANY NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY EURÓPSKEJ ÚNIE 7

5.1. Európsky program na ochranu najdôležitejšej infraštruktúry 7

5.2. Implementácia EPCIP 9

5.3. Ciele EPCIP a ukazovatele pokroku 9

TECHNICKÁ PRÍLOHA 11

1. ÚVOD

Európska rada na svojom zasadnutí v júni 2004 požiadala Komisiu a vysokého predstaviteľa, aby vypracovali celkovú stratégiu na ochranu najdôležitejšej infraštruktúry.

Toto oznámenie poskytuje prehľad činností, ktoré Komisia v súčasnosti vykonáva na ochranu najdôležitejšeji nfraštruktúry a navrhuje dodatočné opatrenia zamerané na posilnenie súčasných nástrojov a splnenie mandátov, ktoré udelila Európska rada.

2. HROZBA

Možnosti pre katastrofické útoky teroristov, ktoré postihujú najdôležitejšiu infraštruktúru, sa zväčšujú. Dôsledky útoku na priemyselné kontrolné systémy najdôležitejšej infraštruktúry môžu kolísať v širokom rozsahu. Všeobecne sa predpokladá, že úspešný elektronický útok by si vyžiadal málo zranení alebo obetí na životoch, ak vôbec nejaké, mohol by však spôsobiť škody na životne dôležitých infraštruktúrnych službách. Napríklad, úspešný elektronický útok na verejnú sieť telefonického spojenia by mohol pripraviť jej užívateľov o telefonické služby, kým technici neobnovia a neopravia spojovaciu sieť. Útok na kontrolné systémy chemických zariadení alebo zariadení kvapalného zemného plynu by mohol spôsobiť oveľa rozsiahlejšie straty na životoch, ako aj značné fyzické škody.

Ďalší druh katastrofického zlyhania infraštruktúry by mohol nastať v prípade, keď jedna časť infraštruktúry vedie k zlyhaniu iných častí a spôsobí rozsiahly kaskádový efekt. K takémuto zlyhaniu by mohlo dôjsť v dôsledku vzájomného synergického efektu infraštruktúrnych odvetví. Jednoduchým príkladom by mohol byť útok na elektrické zariadenia, ktorý by spôsobil prerušenie dodávky elektrického prúdu; aj čistiarne odpadových vôd a vodárne môžu prestať fungovať v prípade vyradenia z prevádzky turbín a inej elektrickej aparatúry v týchto zariadeniach.

Aj kaskádové prípady môžu byť veľmi škodlivé, keďže spôsobujú rozsiahle výpadky zariadení. Výpadky dodávky elektrického prúdu v Severnej Amerike a v Európe počas dvoch posledných rokov jasne preukázali zraniteľnosť energetických infraštruktúr, a teda aj potrebu nájsť efektívne opatrenia na zabránenie a/alebo zmiernenie dôsledkov vyplývajúcich z veľkého prerušenia zásobovania. Toto používanie elektronického terorizmu by mohlo vyústiť aj do zosilnenia účinkov fyzických útokov. Príkladom toho by mohol byť klasický bombový útok na budovu spojený s dočasným prerušením elektrických alebo telefonických služieb. Výsledné zhoršenie núdzového reagovania dovtedy, kým nebudú môcť byť uvedené do činnosti a používané záložné elektrické a komunikačné systémy, by mohlo zvýšiť počet zranení a obetí na životoch, ako aj paniku verejnosti.

3. NAJDÔLEŽITEJŠIE INFRAŠTRUKTÚRY EURÓPY

3.1. Čo je najdôležitejšia infraštruktúra

Najdôležitejšia infraštruktúra pozostáva z tých fyzických a informačno-technologických zariadení, sietí, služieb a majetkových hodnôt, ktorých porušenie alebo zničenie by malo vážny dopad na zdravie, bezpečnosť, istotu a ekonomický blahobyt občanov alebo na efektívne fungovanie vlád v členských štátoch. Najdôležitejšie infraštruktúry sa rozprestierajú

cez mnohé sektory ekonomiky vrátane bankovníctva a financií, dopravy a distribúcie, energetiky, verejnoprospešných služieb, zdravotníctva, zásobovania potravinami a komunikácií, ako aj hlavných orgánov štátnej správy. Niektoré kľúčové prvky v týchto sektoroch nie sú, prísne vzaté, „infraštruktúrnymi“, no fakticky to sú siete alebo zásobovacie reťazce, ktoré podporujú dodávky životne dôležitých výrobkov alebo služieb. Napríklad zásobovanie našich hlavných mestských oblastí potravinami alebo vodou závisí od niekoľkých kľúčových zariadení, ale aj od zložitej siete pestovateľov, spracovateľov, výrobcov, distribútorov a maloobchodníkov.

Najdôležitejšie infraštruktúry zahŕňajú:

- Energetické zariadenia a siete (napr. výroba elektrickej energie, nafty a plynu, skladovacie zariadenia a rafinérie, prenosové a distribučné systémy).

- Komunikačnú a informačnú technológiu (napr. telekomunikácie, televízne a rozhlasové vysielacie systémy, programové a technické prostriedky a siete vrátane internetu)

- Financie (napr. bankovníctvo, cenné papiere a investície)

- Zdravotníctvo (napr. nemocnice, zariadenia zdravotnej starostlivosti a zásobovania krvou, laboratóriá a lekárne, vyhľadávacie a záchranné služby, pohotovosť)

- Potraviny (napr. bezpečnosť, výrobné prostriedky, veľkoobchodná distribúcia a potravinový priemysel)

- Vodu (napr. priehrady, vodné nádrže, čistiarne a siete)

- Dopravu (napr. letiská, prístavy, zariadenia využívajúce rôzne spôsoby dopravy, železnice a hromadné tranzitné siete, systémy riadenia dopravy)

- Výrobu, skladovanie a prepravu nebezpečného tovaru (napr. chemické, biologické, rádiologické a jadrové materiály)

- Štátnu správu (napr. kľúčové služby, zariadenia, informačné siete, majetkové hodnoty a kľúčové štátne pracoviská a pamiatky).

Tieto infraštruktúry vlastní a prevádzkuje tak verejný, ako aj súkromný sektor. Komisia však vo svojom oznámení 574/2001 z 10. októbra 2001 vyhlásila: „Za posilnenie niektorých bezpečnostných opatrení štátnymi orgánmi vzápätí po útokoch namierených proti celej spoločnosti a nie proti priemyselným subjektom musí zodpovedať štát.“ Verejný sektor musí preto zohrávať hlavnú úlohu.

Najdôležitejšie infraštruktúry je potrebné definovať na úrovni členských štátov a na európskej úrovni a tieto zoznamy treba zostaviť do konca roku 2005.

Najdôležitejšie infraštruktúry Európy sú dôkladne prepojené a vzájomne závislé. Konsolidácia spoločností, racionalizácia priemyslu, efektívne obchodné praktiky, ako je spôsob riadenia výroby časovo prispôsobený spotrebe, koncentrácia obyvateľstva v mestských zónach, to všetko prispelo k tejto situácii. Kľúčové infraštruktúry Európy sa stali väčšmi závislými od bežných informačných technológií vrátane internetu a kozmickej rádionavigácie a komunikácie. Cez tieto vzájomne závislé infraštruktúry sa problémy môžu

kaskádovito šíriť, spôsobujúc neočakávané a čoraz vážnejšie poruchy životne dôležitých služieb. Vzájomná prepojenosť a vzájomná závislosť vystavuje tieto infraštruktúry väčšmi narušeniu alebo zničeniu.

Je potrebné skúmať kritériá určovania faktorov, ktoré spôsobujú, že konkrétna infraštruktúra alebo prvok infraštruktúry sa stávajú kľúčovými. Tieto výberové kritériá by sa mali zakladať aj na odvetvovej a kolektívnej odbornosti. Na identifikáciu potenciálnej najdôležitejšej infraštruktúry možno navrhnúť tri faktory:

- Rozsah - Strata prvku najdôležitejšej infraštruktúry sa môže hodnotiť podľa rozsahu zemepisnej oblasti, ktorá môže byť postihnutá jeho stratou alebo nedostupnosťou - medzinárodný, vnútroštátny, krajský/územný alebo miestny.

- Veľkosť - Miera dopadu alebo straty sa môže hodnotiť ako nulová, minimálna, mierna alebo veľká. Medzi kritériá, ktoré by sa mohli použiť na hodnotenie potenciálnej veľkosti, patria:

    (a) dopad na verejnosť (počet postihnutých obyvateľov, straty na životoch, ochorenia, vážne poranenia, evakuácia);

    (b) ekonomické (vplyv na HDP, závažnosť ekonomických strát a/alebo zhoršenie výrobkov alebo služieb);

    (c) environmentálne (dopad na verejnosť a okolitú lokalitu);

    (d) vzájomná závislosť (medzi ostatnými veľmi dôležitými prvkami infraštruktúry); a

    (e) politické (dôvera v schopnosť štátnej správy).

- Vplyv času - Toto kritérium určuje, v akom momente by strata prvku mohla mať vážny dopad (t. j. okamžite, po 24 - 48 hodinách, o týždeň, inokedy).

V mnohých prípadoch však psychologický efekt môže vystupňovať inak zanedbateľné udalosti.

Súčasný vývoj v oblasti ochrany najdôležitejšej infraštruktúry je dokumentovaný v technickej prílohe, ktorá poskytuje odvetvový prehľad výsledkov Komisie, ktoré boli doposiaľ dosiahnuté. Dokazujú, že Komisia získala v tejto oblasti značné skúsenosti.

3.2. Riadenie bezpečnosti

Na analyzovanie hrozby, rozsahu pôsobenia a zraniteľnosti prvkov najdôležitejšej infraštruktúry členských štátov a ich závislostí sú potrebné informácie z viacerých zdrojov. Každý sektor a členský štát bude musieť označiť infraštruktúru, ktorá je pre neho najdôležitejšia, v rámci príslušných jurisdikcií v súlade s harmonizovaným postupom Európskej únie a organizácie alebo osoby poverené bezpečnosťou.

Nie všetky infraštruktúry môžu byť chránené pred všetkými hrozbami. Napríklad elektrické prenosové siete sú príliš veľké, aby mohli byť ohradené alebo strážené. Uplatňovaním postupov spojených s riadením rizík sa môže pozornosť sústrediť na najrizikovejšie oblasti,

zohľadňujúc hrozbu, relatívnu kritickosť, existujúcu úroveň ochrannej bezpečnosti a efektívnosť dostupných zmierňujúcich stratégií pre nepretržitosť činností.

Riadenie bezpečnosti je premyslený proces pochopenia rizík a rozhodovania o implementácii činností na zníženie rizika na stanovenú úroveň, ktorá je akceptovateľnou úrovňou rizika pri akceptovateľnej cene. Tento prístup je charakterizovaný identifikáciou, hodnotením a kontrolou rizík na úrovni, ktorá zodpovedá stanovenej úrovni.

Ochrana najdôležitejšej infraštruktúry (CIP) vyžaduje dôsledné, kooperačné partnerstvo medzi vlastníkmi a prevádzkovateľmi najdôležitejšej infraštruktúry a orgánmi členských štátov. Zodpovednosť za riadenie rizík v rámci fyzických zariadení, zásobovacích reťazcov, informačných technológií a komunikačných sietí spočíva predovšetkým na vlastníkoch a prevádzkovateľoch.

Musia sa vydávať výstrahy, informačné správy a oznámenia s cieľom pomôcť zainteresovaným osobám verejného a súkromného sektora ochrániť kľúčové infraštruktúrne systémy. Z času na čas môžu vznikať osobitné riziká alebo hrozby teroristického útoku, ktoré vyžadujú okamžité reagovanie. V takýchto prípadoch sa bude od vlád a priemyslu členských štátov vyžadovať koordinovaná, operačne sústredená reakcia. Za týchto okolností má Európska únia koordinovať nevyhnutné politické reakcie a na tomto základe budú so zainteresovanými osobami od prípadu k prípadu dohodnuté podrobné podporné mechanizmy.

Aj tie najlepšie plány a právne predpisy na riadenie bezpečnosti, ktoré si vynucujú svoje uplatnenie, sú bezcenné bez správnej implementácie. Skúsenosti svedčia o tom, že nezávislé bezpečnostné inšpekcie ich implementácie vykonávané Komisiou sú jediným účinným nástrojom, ktorý zaručí správnu implementáciu bezpečnostných požiadaviek.

4. POKROK DOSIAHNUTÝ V OCHRANE NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY NA ÚROVNI SPOLOČENSTVA

Európania očakávajú, že najdôležitejšie infraštruktúry budú fungovať ďalej nezávisle od toho, ktoré organizácie vlastnia alebo prevádzkujú ich jednotlivé zložky. Očakávajú, že vlády členských štátov a Európska únia budú zohrávať vedúcu úlohu pri zabezpečovaní takéhoto fungovania. Očakávajú, že štátna správa na všetkých stupňoch bude spolupracovať s vlastníkmi a prevádzkovateľmi zo súkromného sektora, aby sa zabezpečila nepretržitosť služieb, od ktorých Európania závisia.

Ako doplnok k opatreniam, ktoré boli prijaté na vnútroštátnej úrovni, Európska únia už prijala celý rad legislatívnych opatrení stanovujúcich minimálne štandardy na ochranu infraštruktúry v rámci svojich rozličných politík. Platí to najmä v prípade dopravy, komunikácií, energetiky, ochrany zdravia a bezpečnosti pri práci a zdravotníctva. Tieto aktivity sa vystupňovali po nedávnych útokoch v Amerike a Európe. Povedú k ďalšiemu skvalitneniu alebo rozšíreniu existujúcich opatrení.

Inšpekcie sa po celé desaťročia vykonávali v rámci Zmluvy o EURATOM-e s cieľom kontrolovať správne používanie jadrových materiálov. V oblasti ochrany pred žiarením existuje značný počet právnych predpisov, ktoré sa uplatňujú na riziká súvisiace s prevádzkovaním zariadení a používaním zdrojov obsahujúcich rádioaktívne látky.

V oblasti medzinárodnej dopravy Európska únia prijala právne predpisy, ktoré implementujú alebo rozširujú dohody dosiahnuté medzinárodnými riadiacimi orgánmi v sektore leteckej a

námornej dopravy. Európska únia bude naďalej presadzovať svoje aktivity na medzinárodnej úrovni a aktívne sa na nich podieľať. Bude nabádať tretie krajiny, ktoré majú hospodárske vzťahy s Európskou úniou, aby realizovali tieto dohody. Niektorým z nich poskytla určitú pomoc na účel dosiahnutia jednotnej a stálej úrovne bezpečnosti v rámci hraníc i za hranicami EÚ.

Ďalším krokom je zriaďovanie agentúr, ako je Európska agentúra pre bezpečnosť sietí a informácií (EABSI, European Network and Information Security Agency - ENISA), zameraných na bezpečnosť komunikácií. Okrem toho, v sektoroch, ako je bezpečnosť leteckej a námornej dopravy, boli v rámci Komisie zriadené inšpekčné útvary na kontrolu implementácie bezpečnostných právnych predpisov členskými štátmi. Tieto inšpekcie vytvárajú nevyhnutný štandard, ktorý zabezpečuje rovnakú úroveň implementácie v celej Európskej únii.

Súčasný vývoj v ochrane najdôležitejšej infraštruktúry je dokumentovaný v technickej prílohe, ktorá poskytuje odvetvový prehľad výsledkov Komisie, ktoré boli doposiaľ dosiahnuté. Dokazujú, že Komisia získala v tejto oblasti značné skúsenosti.

5. ZVÝŠENIE VÝKONNOSTI OCHRANY NAJDÔLEŽITEJŠEJ INFRAŠTRUKTÚRY EURÓPSKEJ ÚNIE

5.1. Európsky program na ochranu najdôležitejšej infraštruktúry

Majúc na pamäti veľký počet potenciálnych najdôležitejších infraštruktúr a ich osobitosti, nie je možné ochrániť ich všetky opatreniami na európskej úrovni. Pri uplatňovaní zásady subsidiarity musí Európa zamerať svoje úsilie na ochranu infraštruktúr, ktoré majú cezhraničnú pôsobnosť a všetky ostatné ponechať vo výlučnej zodpovednosti členských štátov, ale pod spoločným rámcom.

Už existuje veľký počet smerníc a nariadení, ktoré ustanovujú prostriedky na zisťovanie havárií, zavádzanie plánov zasahovania v spolupráci s civilnou obranou, pravidelné cvičenia a väzby medzi rozličnými úrovňami zasahovania, orgánmi verejnej moci, centrálnymi organizáciami a neodkladnými službami. Na druhej strane však treba ešte veľa urobiť pre ochranu energetických zariadení iných ako jadrové. Ako sa uvádza v technickej prílohe, právne predpisy Spoločenstva v oblasti ochrany najdôležitejších infraštruktúr existujú na rôznom stupni vývoja.

Vo väčšine vyššie uvedených oblastí prebieha práca a spolupráca s expertmi členských krajín a príslušných sektorov ekonomiky zameraná na zisťovanie možných nedostatkov a uplatňovanie nápravných opatrení (právnych alebo iných). Boli vytvorené mnohé siete a bezpečnostné výbory.

Komisia bude v každom kalendárnom roku podávať ostatným inštitúciám správy o pokroku prostredníctvom oznámenia. Pre každý sektor bude analyzovať postup práce spoločenstva v oblasti hodnotenia rizík, vývoja metód ochrany alebo prebiehajúce/plánované právne kroky s cieľom zhromaždiť ich rady. Ďalej v tomto oznámení bude Komisia, v prípade potreby, navrhovať aktualizáciu a horizontálne organizačné opatrenia, ktoré vyžadujú zosúladenie, koordináciu alebo spoluprácu. Toto oznámenie spájajúce sektorové analýzy a opatrenia bude tvoriť základ pre Európsky program na ochranu najdôležitejšej infraštruktúry (EPCIP).

Tento program sa bude snažiť poskytovať pomoc priemyslu a vládam členských štátov na všetkých úrovniach v Európskej únii pri rešpektovaní jednotlivých mandátov a zodpovedností. Komisia je toho názoru, že sieť združujúca odborníkov na CIP z členských štátov EÚ by mohla pomôcť Komisii zostaviť program - táto Varovná informačná sieť najdôležitejšej infraštruktúry (CIWIN) sa má vybudovať čo možno najskôr v roku 2005.

Vytvorenie tejto siete má pomôcť hlavne pri stimulovaní výmeny informácií o spoločných hrozbách a zraniteľnostiach a adekvátnych opatreniach a stratégiách na zmiernenie rizík, ktoré majú prispieť k ochrane najdôležitejšej infraštruktúry. Preto by členské štáty zo svojej strany mali zabezpečiť, aby boli príslušné informácie postúpené všetkým relevantným vládnym rezortom a úradom, vrátane organizácií pohotovostných služieb, informujúc príslušné subjekty priemyselného sektora tak, aby tieto zase informovali postihnutých vlastníkov a prevádzkovateľov najdôležitejšej infraštruktúry cez sieť kontaktov vybudovanú v členských štátoch.

EPCIP by podporil nepretržite prebiehajúce fórum, na ktorom môžu byť obmedzenia hospodárskej súťaže, zodpovednosť a citlivosť informácií vyvážené výhodami bezpečnejšej najdôležitejšej infraštruktúry. Priemysel bude v tomto procese dôkladne konzultovaný. To umožní poskytovať partnerom viac informácií o špecifických hroziacich situáciách, čo im umožní prijať kroky na zabránenie ich možným následkom. Povinnosť a zodpovednosť majiteľov a prevádzkovateľov robiť svoje vlastné rozhodnutia a plány na ochranu svojich vlastných majetkových hodnôt by sa nemala meniť.

Ak neexistujú sektorové normy, alebo ak ešte neboli zavedené medzinárodné predpisy, Európsky výbor pre normalizáciu (CEN) a ďalšie relevantné normalizačné organizácie by mohli pomôcť sieti a navrhnúť jednotné bezpečnostné sektorové a upravené normy pre najrozličnejšie zainteresované odvetvia a sektory. Takéto normy by mali byť navrhnuté aj na medzinárodnej úrovni cestou Medzinárodnej organizácie pre normalizáciu (ISO), aby sa v tomto ohľade vytvorili primerané rovnaké podmienky.

Pri oznamovaní vnútroštátnych bezpečnostných hrozieb pre kľúčovú infraštruktúru, vrátane terorizmu, je nutné postupovať opatrne, aby sa zabránilo vzniku zbytočných obáv medzi obyvateľmi členských štátov EÚ, ako aj potenciálnymi turistami a investormi. Terorizmus je trvalá hrozba, je však úlohou tvorcov politiky nabádať všetkých, aby pokračovali vo svojom živote pokiaľ možno nerušene. Treba sa tiež postarať o to, aby sa zabezpečilo rešpektovanie práv na súkromie tak v Únii, ako aj mimo nej. Spotrebitelia a prevádzkovatelia musia mať istotu, že s informáciami sa bude zaobchádzať precízne, dôverne a spoľahlivo. Je nevyhnutné, aby existoval primeraný systém, ktorý zabezpečí, že dôverné informácie budú riadne spravované a chránené pred neoprávneným použitím a zverejnením.

Mnohé najdôležitejšie infraštruktúry tak Európskej únie, ako aj jej členských štátov, prekračujú hranice Európskej únie. Potrubia sa tiahnu cez kontinenty, káble životne dôležité pre služby informačnej technológie sa ukladajú hlboko do dna oceánov atď. To znamená, že medzinárodná spolupráca je dôležitým komponentom pri vytváraní nepretržitého, dynamického vnútroštátneho a medzinárodného partnerstva medzi vlastníkmi/prevádzkovateľmi najdôležitejších infraštruktúr a vládami tretích krajín, najmä priamymi dodávateľmi produktov energetiky do Únie.

5.2. Implementácia EPCIP

Ochrana najdôležitejšej infraštruktúry vyžaduje aktívnu účasť vlastníkov a prevádzkovateľov infraštruktúry, regulátorov, profesionálnych subjektov a priemyselných združení, ako aj členských štátov a Komisie. Na základe informácií poskytovaných prepojovacími medzičlánkami členských štátov a sieťou, cieľom EPCIP bude pokračovať v identifikácii najdôležitejšej infraštruktúry, analyzovaní zraniteľnosti a vzájomnej závislosti a navrhovať riešenia na ochranu pred všetkými nebezpečenstvami a pripravenosť na ne. To bude zahŕňať pomoc priemyselným sektorom pri uvedomení si hrozby a možných následkov v ich hodnotení rizík. Orgány presadzovania práva v členských štátoch a mechanizmy civilnej ochrany majú zabezpečiť, aby bol EPCIP neoddeliteľnou súčasťou ich plánovania a zvyšovania informovanosti.

Útvary Komisie budú v úzkej spolupráci so sieťou rozvíjať ďalšie činnosti, ktoré majú pozostávať z prijímania právnych predpisov a/alebo šírenia informácií. Jednotka pre zvláštne úlohy policajných prezidentov a Europolu bude musieť zohrávať významnú úlohu pri poskytovaní relevantných informácií o úrovniach bezpečnosti a spravodajských informácií orgánom presadzovania práva v členských štátoch, ktoré zase majú informovať a udržiavať kontakty s vlastníkmi a prevádzkovateľmi najdôležitejšej infraštruktúry v súvislosti s relevantnými informáciami o hrozbe, pomáhať pri poskytovaní informácií o ochrannej bezpečnosti a rozvíjať stratégie ochrannej bezpečnosti na účel boja proti terorizmu.

Vlády členských štátov budú ďalej rozvíjať a/alebo udržiavať databázy vnútroštátne významnej najdôležitejšej infraštruktúry a budú zodpovedné za rozvoj, potvrdzovanie platnosti a audit relevantných plánov, a tak zabezpečovať nepretržitosť služieb v rámci ich jurisdikcií. Pri zavádzaní programu EPCIP bude Komisia predkladať návrhy toho, čo má byť minimálnym obsahom a formátom takýchto databáz a ako majú byť navzájom prepojené.

Vlády členských štátov budú zo svojej strany naďalej poskytovať vlastníkom a prevádzkovateľom najdôležitejšej infraštruktúry (prípadne aj ostatným členským štátom) relevantné spravodajské informácie a výstrahy, ako aj informovať ich o dohodnutých formách reagovania predpokladaných pre každú úroveň hrozby/výstrahy pre zainteresované osoby.

Vlastníci a prevádzkovatelia najdôležitejšej infraštruktúry sa postarajú o adekvátnu bezpečnosť svojich majetkových hodnôt aktívnou implementáciou svojich bezpečnostných plánov a vykonávaním pravidelných inšpekcií, cvičení, hodnotení a plánov. Členské štáty majú kontrolovať celkový proces, zatiaľ čo Komisia má zabezpečiť rovnakú implementáciu adekvátnych inšpekčných systémov v celej Európskej únii.

5.3. Ciele EPCIP a ukazovatele pokroku

Cieľom programu EPCIP a úlohou Komisie bude zabezpečiť existenciu adekvátnych a rovnakých úrovní ochrannej bezpečnosti pre najdôležitejšiu infraštruktúru, minimálnych jednotlivých prípadov zlyhania a rýchlych, testovaných mechanizmov obnovy v celej Európskej únii. Program EPCIP bude nepretržitý proces a bude potrebná jeho pravidelná kontrola, aby sa držal krok s problémami a požiadavkami Spoločenstva.

Úspech je hodnotený podľa:

- identifikácie a vytvorenia zoznamov najdôležitejších infraštruktúr vládami členských štátov v ich jurisdikciách v súlade s prioritami načrtnutými v programe EPCIP;

- spolupráce podnikov v rámci sektorov a s vládou zameranej na zdieľanie informácií a zníženie pravdepodobnosti prípadov spôsobujúcich rozsiahle alebo zdĺhavé narušenie najdôležitejších infraštruktúr;

- rozhodnutí Európskej komisie ustanoviť spoločný prístup k otázkam bezpečnosti najdôležitejších infraštruktúr spoluprácou všetkých zúčastnených verejných a súkromných subjektov.

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.