EUROPOS BENDRIJŲ KOMISIJA

Briuselis, 20.10.2004
KOM(2004) 702 galutinis

KOMISIJOS KOMUNIKATAS
TARYBAI IR EUROPOS PARLAMENTUI

Ypatingos svarbos infrastruktūros objektų apsauga kovojant su terorizmu

TURINYS

1. PRATARMĖ 3

2. GRĖSMĖ 3

3. EUROPOS YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTAI 3

3.1. Kas yra ypatingos svarbos infrastruktūra 3

3.2. Saugumo valdymas 5

4. YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ APSAUGOS SRITYJE PASIEKTA PAŽANGA BENDRIJOS LYGMENIU 6

5. ES YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ APSAUGOS PAJĖGUMO STIPRINIMAS 7

5.1. Europos ypatingos svarbos infrastruktūros objektų apsaugos programa 7

5.2. EPCIP įgyvendinimas 8

5.3. EPCIP tikslai ir pažangos rodikliai 9

TECHNINIS PRIEDAS 10

1. PRATARMĖ

2004 m. birželio mėn. Europos Vadovų Taryba paprašė Komisijos ir Vyriausiojo įgaliotinio parengti bendrą strategiją ypatingos svarbos infrastruktūrai apsaugoti.

Šiame komunikate pateikiama veiksmų, kurių šiuo metu Komisija imasi ypatingos svarbos infrastruktūros objektams apsaugoti, apžvalga ir siūlomos papildomos priemonės, kuriomis būtų galima sustiprinti esamas priemones ir įvykdyti Europos Vadovų Tarybos suteiktus įgaliojimus.

2. GRĖSMĖ

Katastrofiškų teroristinių išpuolių, kurie turėtų poveikio ypatingos svarbos infrastruktūros objektams, galimybė nuolat didėja. Išpuolio prieš ypatingos svarbos infrastruktūros pramonines valdymo sistemas padariniai galėtų būti labai įvairūs. Paprastai daroma prielaida, kad po sėkmingo elektroninio išpuolio žuvusiųjų ar sužeistųjų būtų nedaug, o gal ir iš viso nebūtų, bet galbūt neliktų gyvybiškai svarbios infrastruktūrinės paslaugos. Pavyzdžiui, po sėkmingo elektroninio išpuolio prieš viešojo telefono ryšio perjungiamąjį tinklą klientai turbūt negalėtų naudotis telefono paslauga, kol technikai vėl atkurtų ir sutaisytų perjungiamąjį tinklą. Dėl išpuolio prieš cheminių arba skystų gamtinių dujų įrenginio kontrolės sistemas galėtų žūti gana daug žmonių, taip pat būtų padaryta didelė fizinė žala.

Kitas katastrofiško infrastruktūros sutrikimo atvejis: viena infrastruktūros dalis gali sutrikdyti kitas jos dalis, sukeldama didelį vienas kitą sąlygojantį efektą. Toks sutrikimas galėtų atsirasti dėl sinergetinio infrastruktūrinių pramonės šakų poveikio viena kitai. Paprasčiausiu pavyzdžiu galėtų būti išpuolis prieš elektros tiekimo įmones, kai sutriktų elektros paskirstymas; taigi neveiktų ir nuotekų valymo įrenginiai, ir vandentiekio įmonės, nes sustotų turbinos ir kiti elektros aparatai.

Vienas kitą sąlygojantys įvykiai taip pat gali padaryti daug žalos, plačiu mastu sustabdydami komunalinių paslaugų tiekimą. Nutrūkstantis elektros srovės tiekimas Šiaurės Amerikoje ir Europoje per pastaruosius dvejus metus akivaizdžiai parodė energetikos infrastruktūros objektų pažeidžiamumą, o kartu ir būtinybę ieškoti veiksmingų priemonių, padedančių išvengti didesnio tiekimo sutrikimo padarinių arba juos sušvelninti. Toks elektroninis terorizmas taip pat gali padidinti fizinio išpuolio padarinius. Jo pavyzdžiu galėtų būti paprastas pastato sprogdinimas ir laikinas elektros tiekimo arba telefono ryšio paslaugos nutraukimas. Tokiomis aplinkybėmis vėluotų atitinkamos reagavimo avarijų atveju priemonės, o kol atsirastų ir būtų panaudotos atsarginės elektros ar ryšių sistemos, gali padidėti aukų skaičius ir žmonių panika.

3. EUROPOS YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTAI

3.1. Kas yra ypatingos svarbos infrastruktūra

Ypatingos svarbos infrastruktūros objektai yra tie fiziniai ir informacinės technologijos įrenginiai, tinklai, paslaugos ir turtas, kurių veikimo nutraukimas arba sunaikinimas turėtų didelį poveikį piliečių sveikatai, saugai, saugumui ar ekonominei gerovei arba veiksmingam valstybių narių vyriausybių funkcionavimui. Ypatingos svarbos infrastruktūros objektai

aprėpia daugelį ekonomikos sektorių, įskaitant bankininkystę ir finansus, transportą ir paskirstymą, energetiką, komunalines įmones, sveikatos, maisto tiekimo ir ryšių, taip pat pagrindines vyriausybines paslaugas. Kai kurios šių sektorių ypatingos svarbos sudėtinės dalys, tiksliau sakant, nėra infrastruktūra, bet iš tikrųjų yra tinklai ar tiekimo grandinės, palaikantys gyvybiškai svarbaus produkto ar paslaugos pristatymą. Pavyzdžiui, maisto ar vandens tiekimas svarbiausioms miestų vietovėms priklauso ne tik nuo kai kurių pagrindinių įrenginių, bet ir nuo sudėtingo gamintojų, perdirbėjų, apdirbėjų, platintojų ir mažmenininkų tinklo.

Ypatingos svarbos infrastruktūros objektams priskiriami:

- energetikos įrenginiai ir tinklai (pvz., elektros energijos, naftos ir dujų gamybos, saugyklų ir perdirbimo įmonių, perdavimo ir paskirstymo sistema),

- ryšiai ir informacinės technologijos (pvz., telekomunikacijos, transliavimo sistemos, programinė įranga, aparatūra ir tinklai, įskaitant internetą),

- finansai (pvz., bankininkystė, vertybiniai popieriai ir investicijos),

- sveikatos priežiūra (pvz., ligoninės, sveikatos priežiūros ir kraujo tiekimo įstaigos, laboratorijos ir vaistai, paieška ir gelbėjimas, avarinės tarnybos),

- maistas (pvz., sauga, gamybos priemonės, didmeninis paskirstymas ir maisto pramonė),

- vanduo (pvz., užtvankos, saugyklos, valymas ir tinklai),

- transportas (pvz., oro uostai, uostai, tarprūšinio transporto kompleksai, geležinkelių ir masinio tranzito tinklai, eismo kontrolės sistemos),

- pavojingų prekių (pvz., cheminių, biologinių, radiologinių ir branduolinių medžiagų) gamyba, sandėliavimas ir vežimas,

- vyriausybė (pvz., ypatingos svarbos tarnybos, įrenginiai, informavimo tinklai, turtas ir pagrindinės valstybinės reikšmės vietos ir paminklai).

Šie infrastruktūros objektai priklauso ir viešajam, ir privačiam sektoriui arba ir vieno, ir kito valdomi. 2001 m. spalio 10 d. komunikate 574/2001 Komisija yra pareiškusi, „kad valstybė turi rūpintis valdžios institucijų tam tikrų apsaugos priemonių reaguojant į išpuolius, nukreiptus prieš visuomenę apskritai, o ne komercinės veiklos dalyvius, stiprinimu“. Dėl to viešasis sektorius turi vaidinti pagrindinį vaidmenį.

Ypatingos svarbos infrastruktūros objektai turi būti apibrėžti valstybių narių lygmeniu ir Europos lygmeniu, o tokie sąrašai turėtų būti nustatyti iki 2005 m. pabaigos.

Europos ypatingos svarbos infrastruktūros objektai yra labai tarpusavyje susiję ir labai vienas nuo kito priklauso. Šią padėtį sąlygojo daugelis veiksnių: bendrovių stambinimas, pramonės racionalizavimas, veiksminga verslo praktika, pavyzdžiui, reikiamu laiku organizuojama gamyba, ir gyventojų koncentracija miesto vietovėse Europos ypatingos svarbos infrastruktūros objektai tapo labiau priklausomi nuo bendrų informacinių technologijų, įskaitant internetą ir kosminėje erdvėje įrengtą radijo navigaciją ir ryšius. Problemos gali plisti iš vienos į kitą tarpusavyje susijusią infrastruktūrą, sukeldamos nenumatytus ir tolydžio

rimtesnius gyvybiškai svarbių paslaugų teikimo sutrikimus. Dėl tarpusavio sąsajų ir tarpusavio priklausomumo šios infrastruktūros tampa labiau pažeidžiamos, jas lengviau sutrikdyti arba sunaikinti.

Turi būti išnagrinėti kriterijai, pagal kuriuos nustatomi veiksniai, dėl kurių tam tikra infrastruktūra arba infrastruktūros dalis yra laikomi ypatingos svarbos. Šie atrankos kriterijai turėtų būti grindžiami sektoriaus ir kolektyvine profesionalia patirtimi. Ypatingos svarbos infrastruktūrai nustatyti galėtų būti siūlomi trys kriterijai:

- Mastas – ypatingos svarbos infrastruktūros dalies netektis yra įvertinama pagal geografinės teritorijos, kurią jos netektis ar nebuvimas galėtų paveikti, mastą: tarptautinį, valstybės, provincijos ar teritorijos arba vietos.

- Dydis – poveikio arba netekties laipsnis gali būti įvertinamas kaip nulinis, minimalus, vidutinis arba didelis. Galimam dydžiui įvertinti galėtų būti naudojami šie kriterijai:

    (a) poveikio gyventojams (poveikį patyrusių gyventojų skaičius, gyvybės netekimas, ligos, sunkūs sužeidimai, evakuacija);

    (b) ekonominis (poveikis BVP, ekonominio nuostolio svarba ir (arba) produktų ar paslaugų pablogėjimas);

    (c) poveikio aplinkai (poveikis žmonėms ir aplinkinei vietovei); ir

    (d) tarpusavio priklausomybės (su kitomis ypatingos svarbos infrastruktūros dalimis).

    (e) politinis (pasitikėjimas valdžios pajėgumu);

- Laiko poveikis – pagal šį kriterijų nustatoma, kokiu metu tos dalies netektis galėtų turėti didelį poveikį (pvz., tuojau pat, per 24–48 valandas, vieną savaitę, ilgesnį laiko tarpą).

Tačiau daugeliu atvejų psichologinis poveikis gali sąlygoti šiaip nereikšmingus įvykius.

Dabartiniai ypatingos svarbos infrastruktūros apsaugos pokyčiai aprašyti techninis priede, kuriame apžvelgiami Komisijos pasiekimai atskiruose sektoriuose. Jei rodo, kad Komisija jau yra įgijusi didelę patirtį šioje srityje.

3.2. Saugumo valdymas

Kad būtų galima atlikti grėsmės, incidento ir valstybių narių ypatingos svarbos infrastruktūros dalių bei nuo jų priklausančių objektų pažeidžiamumo analizę, reikia informacijos iš daugelio šaltinių. Pagal atitinkamą jurisdikciją ir ES suderintą formulę kiekvienam sektoriui ir valstybei narei reikės nustatyti, kokia infrastruktūra jiems yra ypatingos svarbos ir kokios organizacijos ar asmenys yra atsakingi už saugumą.

Ne visi infrastruktūros objektai gali būti apsaugoti nuo visų grėsmių. Pavyzdžiui, elektros perdavimo tinklai yra pernelyg dideli, kad juos būtų galima aptverti arba saugoti pasitelkus sargybą. Taikant rizikos valdymo būdus, dėmesį galima sutelkti į didžiausios rizikos sritis, atsižvelgiant į grėsmę, santykinę svarbą, esamą apsaugos lygį ir esamų poveikio sušvelninimo strategijų veiksmingumą verslo tęstinumui.

Saugumo valdymas yra sąmoningas procesas, apimantis rizikos suvokimą ir sprendimų priėmimą bei juos įgyvendinančius veiksmus mažinant riziką iki apibrėžto lygio: priimtinas rizikos lygis – priimtina kaina. Pagal šį požiūrį reikia nustatyti, išmatuoti ir kontroliuoti rizikos veiksnius, išlaikant tokį lygį, kuris atitinka nustatytąjį.

Ypatingos svarbos infrastruktūros apsauga (CIP) reikalauja darnios, linkusios bendradarbiauti ypatingos svarbos infrastruktūros savininkų bei operatorių ir valstybių narių institucijų partnerystės. Atsakomybė už rizikos valdymą pastatuose ar įrenginiuose, tiekimo grandinėse, informacinių technologijų ir ryšio tinkluose pirmiausia tenka savininkams ir operatoriams.

Siekiant padėti viešojo ir privataus sektoriaus atsakingiems asmenims apsaugoti svarbiausias infrastruktūros sistemas turi būti duodami įspėjimai, rengiami patariamieji ir informaciniai raštai. Kartais gali iškilti konkretaus teroristų išpuolio pavojai ar grėsmės, į kuriuos reikia reaguoti nedelsiant. Tokiais atvejais reikės, kad valstybių narių vyriausybės ir pramonė veiktų labai darniai ir tikslingai. Tokiomis aplinkybėmis reikalingos ES politinio reagavimo priemonės bus koordinuojamos, o jomis remiantis kiekvienu konkrečiu atveju su atsakingais asmenimis bus tariamasi dėl papildomų paramos priemonių.

Netgi geriausi saugumo valdymo planai ir teisės aktai, kuriais nustatomas planų vykdymas, yra beverčiai, jei jie nebus tinkamai įgyvendinami. Patirtis rodo, kad nepriklausomi, su jų įgyvendinimu susiję Komisijos atliekami saugumo patikrinimai yra vienintelė veiksminga priemonė, užtikrinanti teisingą saugumo reikalavimų įgyvendinimą.

4. YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ APSAUGOS SRITYJE PASIEKTA PAŽANGA BENDRIJOS LYGMENIU

Europos gyventojai tikisi, kad ypatingos svarbos infrastruktūros objektai ir toliau funkcionuos, nepaisant to, kokioms organizacijoms jų sudedamosios dalys bepriklausytų arba kokios organizacijos jas bevaldytų. Jie tikisi, kad valstybių narių vyriausybės ir ES vaidins vadovaujantį vaidmenį užtikrinant, kad taip ir būtų. Jie tikisi, kad visų lygių valdžia ir privataus sektoriaus savininkai ir operatoriai užtikrins paslaugų, nuo kurių Europos gyventojai priklauso, nenutrūkstamumą.

Papildydama priemones, kurių buvo imtasi valstybių lygmeniu, Europos Sąjunga jau ėmėsi kelių teisės aktų leidybos priemonių, nustatydama minimalius infrastruktūros objektų apsaugos standartus įvairiose ES politikos srityse. Visų pirma reikėtų paminėti transporto, ryšių, energetikos, darbų ir sveikatos saugos bei visuomenės sveikatos sektorius. Veikla nepaprastai suaktyvėjo po neseniai Amerikoje ir Europoje įvykdytų išpuolių. Esamas priemones bus siekiama toliau tobulinti arba išplėsti.

Ištisus dešimtmečius patikrinimai vietoje buvo atliekami pagal Euratomo sutartį siekiant kontroliuoti tinkamą branduolinių medžiagų naudojimą. Radiacinės saugos srityje yra daug teisės aktų, taikomų pavojams, susijusiems su įrenginių eksploatacija ir radioaktyviųjų medžiagų šaltinių naudojimu.

Tarptautinio transporto srityje Europos Sąjunga priėmė teisės aktus, kuriais įgyvendinami ar įtvirtinami tarptautinių vadovaujančių organizacijų susitarimai aviacijos ir jūrų transporto sektoriuose. Europos Sąjunga ir toliau rems jų veiklą ir aktyviai dalyvaus jų tarptautinėje veikloje. Ji skatins trečiąsias šalis, turinčias ekonominių ryšių su ES, įgyvendinti šiuos

susitarimus. Kai kurioms iš jų ES jau suteikė tam tikrą pagalbą, kad saugumo lygis ES ir už jos ribų būtų vienodas ir nuolatinis.

Dar vienas žingsnis buvo žengtas steigiant agentūras, pavyzdžiui, ryšių saugumui skirtą Europos tinklų ir informacijos apsaugos agentūrą (ENISA). Be to, tokiuose sektoriuose, kaip antai aviacija ir jūrų laivybos saugumas, pačioje Komisijoje yra sukurtos atitinkamos tarnybos, tikrinančios kaip valstybės narės įgyvendina saugumą reglamentuojančius teisės aktus. Šios tarnybos nustato būtinas gaires, kurios užtikrina vienodą įgyvendinimo lygį Sąjungoje.

Dabartiniai ypatingos svarbos infrastruktūros objektų apsaugos pokyčiai yra aprašyti techninis priede, kuriame apžvelgiami Komisijos pasiekimai atskiruose sektoriuose. Jei rodo, kad Komisija jau yra įgijusi didelę patirtį šioje srityje.

5. ES YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ APSAUGOS PAJĖGUMO STIPRINIMAS

5.1. Europos ypatingos svarbos infrastruktūros objektų apsaugos programa

Turint omenyje didelį galimų ypatingos svarbos infrastruktūros objektų skaičių ir jų specifiką, apsaugoti juos visus Europos lygmens priemonėmis neįmanoma. Taikydama subsidiarumo principą, Europa turi sutelkti savo pastangas į tarpvalstybinės reikšmės infrastruktūros objektų apsaugą, o kitus palikti tik valstybių narių atsakomybei, bet pagal bendrą sistemą.

Jau yra daug direktyvų ir reglamentų, nustatančių avarijų išaiškinimo būdus, intervencijos planų kūrimą bendradarbiaujant su civiline gynyba, reguliarias pratybas ir aiškius ryšius tarp įvairių intervencijos lygmenų, viešuosius įgaliojimus, centrines organizacijas ir neatidėliotinos pagalbos teikimo tarnybas. Kita vertus, dar daug reikia nuveikti nebranduolinės energetikos įrenginių apsaugos srityje. Kaip parodyta techninis priede, Bendrijos ypatingos svarbos infrastruktūros objektų apsaugos *acquis* yra nevienodo lygio.

Daugumoje minėtų sričių darbas vyksta, o siekiant nustatyti galimus trūkumus ir taikytinas koregavimo (teisines arba kitas) priemones, bendradarbiauja valstybių narių ekspertai ir atitinkami ekonomikos sektoriai. Įsteigta daug tinklų ir saugumo komitetų.

Komisija kiekvienais kalendoriniais metais rengs komunikatą kitoms institucijoms apie pasiektą pažangą. Jame bus analizuojamas Bendrijos atliktas darbas rizikos įvertinimo srityje, apsaugos būdų raida arba teisiniai veiksmai, kurių imamasi arba numatoma imtis, siekiant išgirsti tų institucijų patarimų. Komisija ir toliau šiame komunikate prireikus siūlys naujus pakeitimus ir horizontalias organizacines priemones, kurias reikia derinti, koordinuoti arba kurias vykdant reikia bendradarbiauti. Šis komunikatas, apimdamas visų sektorių analizes ir priemones, sudarys Europos ypatingos svarbos infrastruktūros objektų apsaugos programos (EPCIP) pagrindą.

Tokia programa bus siekiama ES visais lygmenimis padėti pramonei ir valstybių narių vyriausybėms, tuo pačiu metu atsižvelgiant į kiekvienos jų įgaliojimus ir atsakomybę. Komisija yra tos nuomonės, kad rengiant šią programą Komisijai galėtų padėti ES valstybių narių CIA specialistus telkiantis tinklas – šis Ypatingos svarbos infrastruktūros objektų įspėjimo informacinis tinklas (CIWIN) turėtų būti sukurtas kuo greičiau 2005 m.

Tinklo sukūrimas turėtų daugiausia padėti skatinti keitimąsi informacija apie bendras grėsmes ir pažeidžiamumą bei atitinkamas priemones ir strategijas, padedančias sumažinti riziką rūpinantis ypatingos svarbos infrastruktūros objektų apsauga. Dėl to valstybės narės savo ruožtu rūpintųsi, kad atitinkama informacija būtų perduodama visiems atitinkamiems vyriausybės departamentams ir agentūroms, įskaitant avarinių tarnybų organizacijas, informuojančias atitinkamus pramonės sektoriaus darinius, kad jie savo ruožtu informuotų nukentėjusius ypatingos svarbos infrastruktūros savininkus ir operatorius valstybėse narėse sukurtais susižinojimo tinklais.

EPCIP skatintų nuolatinį forumą, siekiant nustatyti ar galima konkurencijos, atsakomybės ir informacijos jautrumo suvaržymų bei naudos, kurią teikia daug saugesni ypatingos svarbos infrastruktūros objektai, pusiausvyra. Šiame procese bus glaudžiai konsultuojamasi su pramonės atstovais. Partneriams bus teikiama daugiau informacijos apie konkrečias grėsmę keliančias situacijas, kuri leistų jiems imtis veiksmų įveikiant galimus padarinius. Savininkų ir operatorių atsakomybė ir atsiskaitomybė priimant savo sprendimus ir planus, skirtus savo pačių turto apsaugai, neturėtų keistis.

Tai atvejais, kai koks nors sektorius neturi standartų arba kai tarptautinės normos dar nėra nustatytos, Europos standartizacijos komitetas (CEN) ir kitos atitinkamos standartizacijos organizacijos galėtų padėti tinklui ir pasiūlyti visoms įvairioms suinteresuotoms pramonės šakoms ir sektoriams vienodus prie atitinkamo sektoriaus pritaikytus saugumo standartus. Siekiant nustatyti šiuo atžvilgiu tinkamas vienodas sąlygas, tokie standartai taip pat turėtų būti siūlomi tarptautiniu lygmeniu per ISO.

Nuorodas į nacionalinio saugumo grėsmes, įskaitant terorizmą, ypatingos svarbos infrastruktūrai reikėtų daryti apdairiai, kad būtų galima išvengti nereikalingo nerimo ES viduje, taip pat siekiant nekelti nerimo turistams ir investuotojams. Terorizmas yra nuolatinė grėsmė, bet politikų uždavinys yra skatinti, kad visi ir toliau gyventų kiek galima netrikdomi. Taip pat reikia pasirūpinti, kad Sąjungoje ir už jos ribų būtų gerbiamos teisės į privatų gyvenimą. Vartotojai ir veiklos vykdytojai turi būti tikri, kad informacija bus tvarkoma kruopščiai, konfidencialiai ir patikimai. Reikia turėti atitinkamą sistemą, galinčią užtikrinti, kad įslaptinta informacija būtų deramai tvarkoma ir saugoma nuo neleistino naudojimo ar atskleidimo.

Didelė ES ir valstybių narių ypatingos svarbos infrastruktūros dalis peržengia ES sienas. Vamzdynai driekiasi per žemynus, informacinės technologijos paslaugoms nepaprastai svarbūs kabeliai yra nutiesti giliai vandenyno dugne ir pan. Tai reiškia, kad tarptautinis bendradarbiavimas yra svarbi veiklos sudedamoji dalis nustatant esamas dinamiškas nacionalines ir tarptautines ypatingos svarbos infrastruktūros objektų savininkų ar operatorių ir trečiųjų šalių vyriausybių, ypač tiesioginių energijos produktų tiekėjų Sąjungai, partnerystes.

5.2. EPCIP įgyvendinimas

Ypatingos svarbos infrastruktūros objektų apsaugai reikalingas aktyvus infrastruktūros savininkų ir operatorių, reguliavimo institucijų, profesinių organizacijų ir pramonės asociacijų bei valstybių narių ir Komisijos dalyvavimas. Remiantis valstybių narių sąsajų ir tinklo teikiama informacija, EPCIP tikslai ir toliau bus – nustatyti ypatingos svarbos infrastruktūrą, analizuoti pažeidžiamumą bei savitarpio priklausomybę ir siūlyti sprendimus, kaip ją apsaugoti nuo visų pavojų ir jiems pasiruošti. Tai reiškia, kad bus siekiama padėti pramonės sektoriams suprasti grėsmę ir padarinių kintamuosius dydžius jų rizikos įvertinimuose.

Valstybių narių teisėsaugos žinybos ir civilinės saugos mechanizmas turėtų užtikrinti, kad EPCIP taptų jų planavimo ir informuotumo didinimo sudedamąją dalimi.

Glaudžiai koordinuodamos su tinklu, Komisijos tarnybos parengs tolesnius veiksmus, kuriuos turėtų sudaryti teisės aktų priėmimas ir (arba) informacijos skleidimas. Policijos vadovų specialios paskirties grupė ir Europolas turėtų vaidinti tam tikrą vaidmenį skleidžiant informaciją apie atitinkamus saugumo lygius ir žvalgybos informaciją valstybių narių teisėsaugos žinyboms, kurios savo ruožtu turėtų palaikyti ryšius su ypatingos svarbos infrastruktūros objektų savininkais ir operatoriais bei jiems atitinkamai pranešti apie grėsmę, padėti teikiant konsultacijas saugumo klausimais ir rengiant pasipriešinti terorizmui skirtas saugumo strategijas.

Valstybių narių vyriausybės toliau rengs ir (arba) sukurs nacionalinės reikšmės ypatingos svarbos infrastruktūros objektų duomenų bazes ir bus atsakingos už atitinkamų planų rengimą, teisinį įforminimą bei tikrinimą, taip užtikrindamos savo jurisdikcijoje esančių tarnybų veiklos tęstinumą. Sudarydama EPCIP, Komisija teiktų pasiūlymus, koks turėtų būti minimalus tokių duomenų bazių turinys bei forma, ir kaip jos turėtų būti tarpusavyje sujungtos.

Valstybių narių vyriausybės savo ruožtu ir toliau praneštų ypatingos svarbos infrastruktūros objektų savininkams ir operatoriams (taip pat prireikus kitoms valstybėms narėms) atitinkamus žvalgybos duomenis ir įspėtų, taip pat praneštų apie sutartą reagavimo tipą pagal kiekvieną grėsmės suinteresuotiems subjektams ar įspėjimo lygį.

Ypatingos svarbos infrastruktūros objektų savininkai ir operatoriai rūpintųsi savo turto tinkamu saugumu aktyviai įgyvendindami savo saugumo planus ir reguliariai vykdydami patikrinimus, pratybas, įvertinimus ir planus. Valstybės narės kontroliuotų bendrą procesą, o Komisija užtikrintų atitinkamų patikrinimo sistemų vienodą įgyvendinimą visoje Sąjungoje.

5.3. EPCIP tikslai ir pažangos rodikliai

EPCIP tikslas ir Komisijos pareiga būtų visoje Sąjungoje užtikrinti tinkamus ir vienodus ypatingos svarbos infrastruktūros objektų apsaugos lygius, nustatyti minimalius pavienius nesėkmės taškus ir greitas, išbandytas atkūrimo priemones. EPCIP įgyvendinimas būtų nenutrūkstantis procesas, ir ją reikėtų reguliariai peržiūrėti, atsižvelgiant į Bendrijoje iškylančius klausimus ir problemas.

Sėkmė turi būti matuojama atsižvelgiant į tai, kaip:

- valstybių narių vyriausybės identifikuoja ir nustato savo jurisdikcijoje esančių ypatingos svarbos infrastruktūros objektų inventorių pagal EPCIP parengtus prioritetus;

- verslo įmonės bendradarbiauja savo sektoriuose ir su vyriausybe dalindamosi informacija ir mažina incidentų, sukeliančių didelės apimties arba ilgalaikį ypatingos svarbos infrastruktūros objektų sutrikimą, tikimybę;

- ryžtingai Europos bendrija kurs bendrą požiūrį į ypatingos svarbos infrastruktūros objektų saugumo klausimų sprendimą bendradarbiaujant visiems viešojo ir privataus sektorių atstovams.

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.