KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 12.12.2006
KOM(2006) 787 wersja ostateczna

2006/0276 (CNS)

Wniosek

DYREKYWA RADY

w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony

(przedstawiona przez Komisję)

{SEK(2006) 1648}
{SEK(2006) 1654}

UZASADNIENIE

1) KONTEKST WNIOSKU

- **Podstawa i cele wniosku**

Rada Europejska na posiedzeniu w czerwcu 2004 r. zwróciła się do Komisji o opracowanie ogólnej strategii ochrony infrastruktury krytycznej. W dniu 20 października 2004 r. Komisja przyjęła komunikat w sprawie ochrony infrastruktury krytycznej w walce z terroryzmem, w którym zawarto propozycje usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, a także zwiększenia gotowości i zdolności reagowania na takie ataki.

W konkluzjach Rady dotyczących zapobiegania, gotowości i reagowania na ataki terrorystyczne oraz w solidarnościowym programie UE na rzecz przeciwdziałania zagrożeniom i atakom terrorystycznym, przyjętym przez Radę w grudniu 2004 r. Rada poparła inicjatywę Komisji zmierzającą do przedstawienia europejskiego programu ochrony infrastruktury krytycznej (EPOIK) oraz wyraziła zgodę na utworzenie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (SOZIK).

W listopadzie 2005 r. Komisja przyjęła zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej (EPOIK), w której opisano opcje polityczne, jakie Komisja mogłaby zastosować przy opracowywaniu EPOIK i SOZIK.

W grudniu 2005 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (WSiSW) wezwała Komisję do przygotowania do czerwca 2006 r. wniosku legislacyjnego w sprawie EPOIK.

Niniejszy wniosek dotyczący dyrektywy przedstawia środki, jakie Komisja proponuje zastosować w dziedzinie rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz oceny potrzeb w zakresie zwiększenia ich ochrony.

- **Kontekst ogólny**

W Unii Europejskiej istnieje wiele infrastruktur krytycznych, których zakłócenie lub zniszczenie wywołałoby negatywne skutki w więcej niż jednym państwie członkowskim. Może się też zdarzyć, że awaria infrastruktury krytycznej w jednym państwie członkowskim powoduje negatywne skutki w innym. Należy rozpoznać tego rodzaju infrastruktury krytyczne o wymiarze transgranicznym i przyznać im miano europejskich infrastruktur krytycznych. (EIK). Można to zrobić jedynie poprzez wprowadzenie wspólnej procedury rozpoznawania europejskich infrastruktur krytycznych i oceny potrzeb w zakresie zwiększenia ich ochrony.

Ze względu na transgraniczny wymiar rozpatrywanego zagadnienia spójna ogólnoeuropejska koncepcja badania słabości i „czułych miejsc" infrastruktur oraz rozpoznawania luk w ich zabezpieczeniach byłaby przydatnym uzupełnieniem, a zarazem wzbogaceniem działających już w państwach członkowskich krajowych programów ochrony infrastruktury krytycznej, stanowiąc jednocześnie ważne wzmocnienie europejskiego rynku wewnętrznego pod względem jego zdolności utrzymywania rentowności i pomnażania majątku.

Poszczególne sektory charakteryzują się typowymi dla siebie doświadczeniami, wiedzą i wymaganiami dotyczącymi ochrony infrastruktury krytycznej (OIK), dlatego unijna koncepcja OIK powinna być opracowywana i wdrażana z uwzględnieniem specyfiki uwarunkowań infrastruktury krytycznej każdego z tych sektorów; powinna także opierać się na dotychczas stosowanych, właściwych dla danego sektora środkach. Istnieje potrzeba sporządzenia wykazu sektorów infrastruktury krytycznej, aby ułatwić przyjęcie podejścia opartego na indywidualnym traktowaniu sektorów w kontekście ochrony infrastruktury krytycznej.

- **Potrzeba stworzenia wspólnych ram regulacyjnych**

Jedynie wspólne ramy regulacyjne mogą zapewnić konieczną podstawę spójnego i jednolitego procesu wdrażania działań służących zwiększeniu ochrony EIK i tylko dzięki nim możliwe jest wyraźne określenie zakresu odpowiedzialności poszczególnych uczestników tego procesu. Niewiążące, dobrowolne środki, chociaż elastyczne, nie stanowiłyby dostatecznie mocnego fundamentu, gdyż nie dawałyby wystarczającej jasności, kto za co odpowiada ani nie precyzowałyby praw i obowiązków zaangażowanych stron.

Procedury rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz wspólną koncepcję oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur można ustanowić jedynie w drodze dyrektywy, gdyż tylko taki środek zapewni:

- odpowiedni poziom ochrony EIK;
- podobne prawa i obowiązki dla wszystkich podmiotów zaangażowanych w sprawy EIK;
- utrzymanie stabilności rynku wewnętrznego.

Uszkodzenie lub utrata części infrastruktury w jednym państwie członkowskim może mieć negatywny wpływ na kilka innych państw i na gospodarkę europejską w ogóle. Staje się to coraz bardziej prawdopodobne, ponieważ nowe technologie (np. Internet) i liberalizacja rynku (np. w dziedzinie dostaw gazu i energii elektrycznej) sprawiają, że wiele składników infrastruktury stanowi część większej sieci. W takiej sytuacji środki zabezpieczające są tylko tak mocne, jak mocne jest ich najsłabsze ogniwo. Oznacza to, że konieczne może się okazać ustalenie wspólnego poziomu ochrony.

- **Dialog sektorowy z zainteresowanymi stronami**

Skuteczna ochrona wymaga komunikacji, koordynacji i współpracy wszystkich zainteresowanych stron na poziomie poszczególnych krajów i na poziomie UE.

Duże znaczenie ma pełne zaangażowanie sektora prywatnego, gdyż infrastruktura krytyczna należy w większości do podmiotów prywatnych i przez takie podmioty jest obsługiwana. Każdy operator musi kontrolować sposób zarządzania ryzykiem, gdyż to właśnie do niego należy zazwyczaj decyzja o tym, jakie zastosować środki zabezpieczające i plany zachowania ciągłości działania. Przy tworzeniu takich planów należy respektować normalne procesy gospodarcze i kierować się logiką, a przyjęte rozwiązania powinny w miarę możliwości opierać się na standardowych umowach handlowych.

Każdy sektor ma swoje specyficzne doświadczenia, wiedzę i wymagania w dziedzinie ochrony własnej infrastruktury krytycznej.

Dlatego zgodnie z opiniami wyrażonymi w odpowiedzi na zieloną księgę w sprawie EPOIK unijna koncepcja powinna zakładać pełne zaangażowanie sektora prywatnego, uwzględniając przy tym specyfikę poszczególnych sektorów i opierając się na dotychczas stosowanych, właściwych dla danego sektora środkach.

- **Obowiązujące przepisy w dziedzinie, której dotyczy wniosek**

Na poziomie UE nie istnieją obecnie żadne przepisy horyzontalne w dziedzinie ochrony infrastruktury krytycznej. Niniejsza dyrektywa ustanawia procedury rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz wspólne zasady oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur.

Istnieje szereg środków o zasięgu sektorowym, wśród nich:

- w sektorze informatycznym:

  (a) dyrektywa w sprawie usługi powszechnej (2002/22/WE) dotycząca między innymi integralności publicznych sieci łączności elektronicznej;

  (b) dyrektywa w sprawie zezwoleń (2002/20/WE) dotycząca między innymi integralności publicznych sieci łączności elektronicznej;

  (c) dyrektywa o prywatności i łączności elektronicznej (2002/58/WE) dotycząca między innymi bezpieczeństwa publicznych sieci łączności elektronicznej;

  (d) decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne;

  (e) rozporządzenie (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji;

- w sektorze ochrony zdrowia:

  (a) decyzja 2119/98/WE Parlamentu Europejskiego i Rady z dnia 24 września 1998 r. ustanawiająca sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie.

  (b) dyrektywa Komisji 2003/94/WE z dnia 8 października 2003 r. ustanawiająca zasady i wytyczne dobrej praktyki wytwarzania w odniesieniu do produktów leczniczych przeznaczonych dla ludzi oraz produktów leczniczych stosowanych u ludzi, znajdujących się w fazie badań;

- w sektorze finansowym:

  (a) dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych (MiFID);

  (b) ogólne standardy systemów płatności detalicznych w euro przyjęte w czerwcu 2003 r. przez Radę Prezesów Europejskiego Banku Centralnego (EBC);

  (c) dyrektywa 2006/48/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. w sprawie podejmowania i prowadzenia działalności przez instytucje kredytowe;

  (d) dyrektywa 2006/49/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. w sprawie adekwatności kapitałowej firm inwestycyjnych i instytucji kredytowych;

  (e) wniosek dotyczący dyrektywy w sprawie usług płatniczych na rynku wewnętrznym zmieniającej dyrektywy 97/7/WE, 2000/12/WE i 2002/65/WE (KOM(2005) 603);

  (f) dyrektywa 2000/46/WE Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością

  (g) dyrektywa 1998/26/WE Parlamentu Europejskiego i Rady z 19 maja 1998 r. w sprawie zamknięcia rozliczeń;

- w sektorze transportowym:

  (a) rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych;

  (b) rozporządzenie Komisji (WE) nr 884/2005 z dnia 10 czerwca 2005 r. ustanawiające procedury prowadzania inspekcji Komisji w zakresie ochrony żeglugi i portów;

  (c) dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów;

  (d) rozporządzenie (WE) nr 2320/2002 Parlamentu Europejskiego i Rady z dnia 16 grudnia 2002 r. ustanawiające wspólne zasady w dziedzinie bezpieczeństwa lotnictwa cywilnego;

  (e) rozporządzenie Komisji (WE) nr 622/2003 z dnia 4 kwietnia 2003 r. ustanawiające środki w celu wprowadzenia w życie wspólnych podstawowych standardów dotyczących bezpieczeństwa lotnictwa cywilnego;

(f) rozporządzenie Komisji (WE) nr 1217/2003 z dnia 4 lipca 2003 r. ustanawiające wspólne specyfikacje dla krajowych programów kontroli jakości bezpieczeństwa w lotnictwie cywilnym;

(g) rozporządzenie Komisji (WE) nr 1486/2003 z dnia 22 sierpnia 2003 r. ustanawiające procedury przeprowadzania inspekcji Komisji w dziedzinie bezpieczeństwa lotnictwa cywilnego;

(h) rozporządzenie Komisji (WE) nr 68/2004 z dnia 15 stycznia 2004 r. zmieniające rozporządzenie (WE) nr 622/2003 ustanawiające środki w celu wprowadzenia w życie wspólnych podstawowych standardów dotyczących bezpieczeństwa lotnictwa cywilnego;

(i) rozporządzenie (WE) nr 849/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. zmieniające rozporządzenie (WE) nr 2320/2002 ustanawiające wspólne zasady w dziedzinie bezpieczeństwa lotnictwa cywilnego;

(j) rozporządzenie Komisji (WE) nr 1138/2004 z dnia 21 czerwca 2004 r. ustanawiające wspólną definicję części krytycznych stref zastrzeżonych w portach lotniczych;

(k) rozporządzenie Komisji (WE) nr 781/2005 z dnia 24.05.2005 r. zmieniające rozporządzenie (WE) nr 622/2003 ustanawiające środki w celu wprowadzenia w życie wspólnych podstawowych standardów dotyczących bezpieczeństwa lotnictwa cywilnego;

(l) rozporządzenie Komisji (WE) nr 857/2005 z dnia 6 czerwca 2005 r. zmieniające rozporządzenie (WE) nr 622/2003 ustanawiające środki w celu wprowadzenia w życie wspólnych podstawowych standardów dotyczących bezpieczeństwa lotnictwa cywilnego;

(m) dyrektywa 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej;

(n) transport towarów niebezpiecznych reguluje dyrektywa 96/49/WE (zmieniona dyrektywą 2004/110/WE przyjmującą RID 2005);

(o) Konwencja o ochronie fizycznej materiałów jądrowych (podpisanie – 1980 r., przystąpienie – 1981 r., wejście w życie – 1987 r.);.

- w sektorze chemicznym:

(a) niebezpieczne instalacje wg dyrektywy Seveso II (dyrektywy Rady 96/82/WE z dnia 9 grudnia 1996 r. w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi [dyrektywy Seveso II] zmienionej dyrektywą Parlamentu Europejskiego i Rady 2003/105/WE z dnia 16 grudnia 2003 r.);

- w sektorze jądrowym:

  (a) dyrektywa Rady 89/618/Euratom z dnia 27 listopada 1989 r. w sprawie informowania ogółu społeczeństwa o środkach ochrony zdrowia, które będą stosowane oraz działaniach, jakie należy podjąć w przypadku pogotowia radiologicznego;

  (b) decyzja Rady 87/600/Euratom z dnia 14 grudnia 1987 r. w sprawie wspólnotowych warunków wczesnej wymiany informacji w przypadku pogotowia radiologicznego.

- **Spójność z innymi politykami i celami Unii**

Niniejszy wniosek jest całkowicie zgodny z unijnymi celami, szczególnie zaś z dążeniem do „utrzymania i rozwijania Unii jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której zagwarantowana jest swoboda przepływu osób, w powiązaniu z właściwymi środkami w odniesieniu do kontroli granic zewnętrznych, azylu, imigracji oraz zapobiegania i zwalczania przestępczości".

Wniosek ten jest także spójny z polityką w innych dziedzinach, gdyż jego celem nie jest zastępowanie istniejących środków, lecz ich uzupełnienie w celu zwiększenia ochrony EIK.

2) KONSULTACJE Z ZAINTERESOWANYMI STRONAMI I OCENA SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

W kwestiach związanych z opracowaniem EPOIK zasięgnięto opinii wszystkich zainteresowanych stron. Płaszczyzną konsultacji były:

- Zielona księga w sprawie EPOIK, przyjęta 17 listopada 2005 r., z okresem konsultacji do 15 stycznia 2006 r. Swoje opinie zgłosiło 22 państwa członkowskie. Uwagi w sprawie zielonej księgi nadesłało także około 100 przedstawicieli sektora prywatnego. W opiniach tych wyrażano przeważnie poparcie dla idei stworzenia EPOIK.

- Trzy seminaria poświęcone ochronie infrastruktury krytycznej, których gospodarzem była Komisja (w czerwcu 2005 r., wrześniu 2005 r. i marcu 2006 r.). We wszystkich trzech seminariach brali udział przedstawiciele państw członkowskich. Osoby reprezentujące sektor prywatny zaproszono na seminaria we wrześniu 2005 r. i marcu 2006 r.

- Nieformalne spotkania punktów kontaktowych ds. OIK. Komisja zorganizowała dwa spotkania z udziałem przedstawicieli punktów kontaktowych ds. OIK z państw członkowskich (grudzień 2005 r. i luty 2006 r.).

- Nieformalne spotkania z przedstawicielami sektora prywatnego. Zorganizowano liczne nieformalne spotkania z przedstawicielami konkretnych przedsiębiorstw, jak również z przedstawicielami stowarzyszeń branżowych.

- W samej Komisji prace nad opracowaniem EPOIK postępowały dzięki regularnym spotkaniom podgrupy ds. ochrony infrastruktury krytycznej wyłonionej z międzydepartamentalnej grupy ds. wewnętrznych aspektów terroryzmu.

- **Gromadzenie i wykorzystanie wiedzy specjalistycznej**

Potrzebną wiedzę fachową zebrano dzięki licznym spotkaniom i seminariom zorganizowanym w 2004, 2005 i 2006 r., a także w wyniku konsultacji na temat zielonej księgi ws. EPCIP. Informacje pochodziły od wszystkich zainteresowanych stron.

- **Ocena skutków**

Ocenę skutków EPOIK zamieszczono w załączeniu.

3) PRAWNE ASPEKTY WNIOSKU

- **Streszczenie proponowanych działań**

Proponuje się stworzenie zbioru zasad regulujących rozpoznawanie i wyznaczanie europejskich infrastruktur krytycznych oraz oceny potrzeb w zakresie zwiększenia ich ochrony.

- **Podstawa prawna**

Podstawą prawną wniosku jest art. 308 Traktatu ustanawiającego Wspólnotę Europejską.

- **Zasada pomocniczości**

Spełniona jest zasada pomocniczości, gdyż pojedyncze państwo członkowskie UE nie może osiągnąć celów, jakim służą środki podejmowane na mocy niniejszego wniosku, a w związku z tym konieczne jest działanie na poziomie UE. W prawdzie każde państwo członkowskie samo odpowiada za ochronę infrastruktury krytycznej na własnym terytorium, ale z punktu widzenia bezpieczeństwa Unii Europejskiej bardzo ważne jest, by infrastruktura mająca znaczenie dla dwóch lub więcej państw członkowskich albo taka, która ma znaczenie dla danego państwa członkowskiego, lecz zlokalizowana jest w innym, była w wystarczającym stopniu chroniona, i aby jedno lub kilka państw członkowskich nie było narażonych na niebezpieczeństwo z powodu słabości lub niższych norm bezpieczeństwa w innym państwie członkowskim. Istnienie podobnych zasad w dziedzinie bezpieczeństwa jest gwarancją zgodności z regułami konkurencji na rynku wewnętrznym.

- **Zasada proporcjonalności**

Niniejszy wniosek nie wykracza ponad to, co konieczne do osiągnięcia jego głównego celu, czyli zwiększenia ochrony europejskiej infrastruktury krytycznej. Do podstawowych założeń wniosku należy stworzenie podstawowego mechanizmu koordynacyjnego na poziomie UE, zobowiązanie państw członkowskich do rozpoznania swoich infrastruktur krytycznych, wprowadzenie szeregu środków zabezpieczających infrastrukturę krytyczną i wreszcie rozpoznanie i wyznaczenie najważniejszych europejskich infrastruktur krytycznych. We wniosku określa się zatem minimalną liczbę wymogów niezbędnych do rozpoczęcia prac nad zwiększeniem ochrony infrastruktur krytycznych. Celu tego nie da się w pełni osiągnąć

innymi środkami, mianowicie poprzez przyjęcie w odniesieniu do EPOIK podejścia opartego na wytycznych, gdyż nie dawałoby to całkowitej pewności, że nastąpi podniesienie poziomu ochrony w całej UE i nie zapewniłoby pełnego udziału wszystkich zainteresowanych stron.

- **Wybór instrumentów**

Państwa członkowskie mają różne koncepcje ochrony infrastruktury krytycznej i różne systemy prawne. Dlatego najodpowiedniejszym środkiem osiągnięcia wymienionych celów jest dyrektywa, pozwalająca na stworzenie wspólnych procedur rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz wypracowanie wspólnej koncepcji oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur.

4) SKUTKI DLA BUDŻETU

Wpływ proponowanej regulacji na budżet przedstawiono w załączonej do niniejszego wniosku ocenie skutków finansowych.

Program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innych zagrożeń dla bezpieczeństwa" na lata 2007–2013, będący częścią szerszego programu pod nazwą „Bezpieczeństwo i ochrona swobód", przyczyni się do wdrożenia niniejszej dyrektywy, wpływając na wzmocnienie ochrony osób oraz tych zasobów materialnych, usług, sprzętu informatycznego, sieci i składników infrastruktury, których zakłócenie lub zniszczenie miałoby poważny wpływ na podstawowe funkcje społeczne.

Program ten nie odnosi się do spraw, które są objęte zakresem działania innych instrumentów finansowych, szczególnie instrumentu szybkiego reagowania w przypadku poważnych sytuacji kryzysowych i unijnego funduszu solidarnościowego.

5) DODATKOWE INFORMACJE

- **Uchylenie obowiązujących przepisów**

Żadne z obowiązujących przepisów nie wymagają uchylenia.

- **Szczegółowe wyjaśnienie wniosku**

Artykuł 1 – przedstawienie tematyki dyrektywy. W dyrektywie określa się wspólną procedurę rozpoznawania i wyznaczania europejskich infrastruktur krytycznych, to znaczy takich, których zakłócenie lub zniszczenie miałoby negatywny wpływ na co najmniej dwa państwa członkowskie lub na jedno państwo członkowskie, gdy infrastruktura krytyczna jest zlokalizowana w innym państwie członkowskim. Dyrektywa wprowadza także wspólną koncepcję oceny potrzeb w zakresie zwiększenia ochrony europejskich infrastruktur krytycznych. Ocena taka pomoże w przygotowaniu konkretnych środków zabezpieczających dla poszczególnych sektorów OIK.

Artykuł 2 – przedstawienie podstawowych definicji właściwych dla tej dyrektywy.

Artykuł 3 – przedstawienie procedury rozpoznawania EIK. EIK oznacza te infrastruktury krytyczne, których zakłócenie lub zniszczenie miałoby negatywny wpływ na co najmniej dwa państwa członkowskie lub na jedno państwo członkowskie, gdy infrastruktura krytyczna jest

zlokalizowana w innym państwie członkowskim. Procedura ta opiera się na procesie trójstopniowym. Najpierw Komisja razem z państwami członkowskimi i zainteresowanymi stronami opracowuje przekrojowe i sektorowe kryteria rozpoznawania EIK, które zostają następnie przyjęte w procedurze komitologii. Kryteria przekrojowe uzależnia się od rozmiaru strat, jakie powstałyby w następstwie zakłócenia lub zniszczenia danej infrastruktury krytycznej. Rozmiar strat w wyniku zakłócenia lub zniszczenia danej infrastruktury należy w miarę możliwości oceniać na podstawie:

- skutków społecznych (liczba dotkniętych mieszkańców);
- skutków ekonomicznych (wielkość strat ekonomicznych i/lub wartość utraconych towarów lub usług);
- skutków ekologicznych;
- skutków politycznych;
- skutków psychologicznych;
- konsekwencji dla zdrowia publicznego.

Każde państwo członkowskie rozpoznaje następnie infrastruktury, które spełniają te kryteria i zgłasza je Komisji. Rozpoczęto już prace w priorytetowych sektorach OIK wybieranych corocznie spośród sektorów wymienionych w załączniku I. Wykaz sektorów OIK podany w załączniku I można zmieniać za pośrednictwem procedury komitologii o tyle, o ile nie powoduje to rozszerzenia zakresu dyrektywy. Oznacza to w szczególności, że zmiany w wykazie będą służyć doprecyzowaniu jego treści. Zdaniem Komisji do sektorów wymagających najpilniejszych działań należą transport i energia.

Artykuł 4 – określenie procedury wyznaczania EIK. Po zakończeniu procedury określonej w art. 3 Komisja przygotowuje wykaz europejskich infrastruktur krytycznych. Wstępna wersja takiego wykazu opiera się na zgłoszeniach uzyskanych od państw członkowskich i innych dostępnych informacjach. Wykaz taki przyjmuje się następnie w procedurze komitologii.

Artykuł 5 – plany bezpieczeństwa infrastruktury (PBI) Artykuł 5 wymaga od wszystkich właścicieli/operatorów infrastruktur krytycznych zakwalifikowanych jako EIK opracowania PBI, w którym określone zostaną składniki danej infrastruktury i rozwiązania służące ich właściwej ochronie. W załączniku II wymieniono elementy, które muszą się znaleźć w takich planach. Są to między innymi:

- rozpoznanie ważnych składników infrastruktury;
- analiza ryzyka oparta na scenariuszach poważnych zagrożeń, analiza słabych stron poszczególnych składników infrastruktury i analiza potencjalnych skutków;
- rozpoznanie, selekcja i ustalenie hierarchii ważności środków przeciwdziałania i procedur z podziałem na:
    - **Stałe środki bezpieczeństwa**, określające niezbędne inwestycje i środki w dziedzinie bezpieczeństwa, które nie mogą zostać zainstalowane przez właściciela/operatora w krótkim czasie. W tej części planu znajdą się informacje

dotyczące środków ogólnych; środków technicznych (w tym instalacja urządzeń wykrywających, kontrola dostępu, środki zabezpieczające i zapobiegawcze); środki organizacyjne (w tym procedury sygnalizowania zagrożeń i zarządzania kryzysowego); środki kontrolno-weryfikacyjne; komunikacja; podnoszenie świadomości społecznej i szkolenia oraz bezpieczeństwo systemów informacyjnych.

- **Doraźne środki bezpieczeństwa**, które uruchamia się w zależności od zmieniającego się poziomu ryzyka i zagrożenia.

Każdy sektor OIK może opracować indywidualny, dostosowany do własnych potrzeb PBI oparty na minimalnych wymogach wymienionych w załączniku 2. Plany takie przyjmuje się w procedurze komitologii.

Dla sektorów, w których istnieją już podobne obowiązki, art. 5 ust. 2 przewiduje możliwość zwolnienia z wymogu sporządzania PBI na podstawie decyzji podjętej w procedurze komitologii. Uznaje się, że dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów gwarantuje spełnienie wymogu opracowania planów bezpieczeństwa infrastruktury w tej dziedzinie.

Po stworzeniu PBI każdy właściciel/operator EIK powinien przedstawić go odpowiedniemu organowi państwa członkowskiego. Każde państwo członkowskie ustanowi system nadzoru realizacji PBI, dzięki któremu właściciel/operator EIK uzyska informacje zwrotne na temat jakości PBI, a zwłaszcza prawidłowości ocen ryzyka i zagrożeń.

Artykuł 6 – urzędnik łącznikowy ds. bezpieczeństwa (UŁB). Artykuł 6 nakłada na wszystkich właścicieli/operatorów infrastruktur krytycznych zakwalifikowanych jako EIK obowiązek wyznaczenia UŁB. Urzędnik taki pełniłby rolę skrzynki kontaktowej w sprawach związanych z bezpieczeństwem dla właścicieli/operatorów EIK i odpowiednich organów ds. OIK w państwach członkowskich. UŁB otrzymywałby zatem od organów państw członkowskich wszystkie istotne informacje związane z OIK oraz byłby odpowiedzialny za przekazywanie państwom członkowskim informacji pochodzących od właścicieli/operatorów EIK.

Artykuł 7 – sprawozdawczość. Artykuł 7 wprowadza szereg środków w zakresie sprawozdawczości. Każde państwo członkowskie jest zobowiązane do prowadzenia oceny ryzyka i zagrożenia dla EIK. Informacje uzyskane w trakcie takich analiz stanowią podstawę dialogu państw członkowskich z właścicielami/operatorami EIK na tematy związane z bezpieczeństwem (nadzoru), o którym mowa w art. 5. W związku z tym, że art. 5 nakłada na właścicieli/operatorów EIK obowiązek sporządzania planów bezpieczeństwa infrastruktury i przedstawiania ich organom państw członkowskich, każde państwo członkowskie prosi się o opracowanie ogólnego zestawienia słabych stron, rodzajów zagrożeń i ryzyka charakterystycznych dla każdego z sektorów OIK oraz o przekazanie takich informacji Komisji. Posłużą one Komisji jako podstawa przy ocenianiu, czy potrzebne są dodatkowe środki zabezpieczające. Te same informacje można wykorzystać później do opracowania ocen skutków, które będą towarzyszyć przyszłym wnioskom legislacyjnym w tej dziedzinie.

Artykuł ten przewiduje także opracowanie wspólnych metod oceny ryzyka, zagrożeń i słabych stron w odniesieniu do EIK. Metody takie przyjmowanoby w procedurze komitologii.

Artykuł 8 – Wsparcie dla właścicieli/operatorów EIK. Komisja udzieli właścicielom/operatorom EIK wsparcia polegającego na udostępnieniu im najlepszych

praktyk i metod związanych z OIK. Podejmie się zadania gromadzenia takich informacji z różnych źródeł (np. państwa członkowskie, źródła własne) i udostępniania ich wszystkim zainteresowanym.

Artykuł 9 – punkty kontaktowe ds. OIK. W trosce o właściwą współpracę i koordynację działań związanych z OIK każde państwo członkowskie jest zobowiązane do wyznaczenia punktu kontaktowego ds. OIK. Punkt kontaktowy koordynowałby sprawy związane z OIK w obrębie danego państwa członkowskiego, a także odpowiadał za współpracę w tym względzie z innymi państwami członkowskimi i Komisją.

Artykuł 10 – poufność i wymiana informacji dotyczących OIK. Poufność i wymiana informacji dotyczących OIK to ważny i delikatny element w pracy nad OIK. W związku z tym dyrektywa nakłada na Komisje i państwa członkowskie obowiązek podejmowania odpowiednich środków w celu ochrony informacji. Personel odpowiedzialny za przetwarzanie zastrzeżonych informacji dotyczących OIK powinien podlegać specjalnej kontroli organów państwa członkowskiego.

Artykuł 11 – Komitet. Niektóre przepisy dyrektywy zostaną wprowadzone w drodze procedury komitologii. Komitet będzie się składał z osób działających w punktach kontaktowych. W odniesieniu do zwolnienia niektórych sektorów z obowiązku sporządzania PBI, o czym mowa w art. 5 ust. 2, wykorzystana zostanie procedura doradcza.

Procedurę regulacyjną przewiduje się zastosować dla następujących kwestii:

- Artykuł 3 ust. 1 – przyjęcie przekrojowych i sektorowych kryteriów rozpoznawania EIK
- Artykuł 3 ust. 2 – zmiana wykazu sektorów OIK podanego w załączniku 1
- Artykuł 4 ust. 2 – przyjęcie wstępnego wykazu sektorów OIK
- Artykuł 5 ust. 2 – opracowanie wymogów sektorowych dotyczących PBI
- Artykuł 7 ust. 2 – opracowanie wspólnego modelu ogólnych sprawozdań dotyczących rozpoznanych zagrożeń, ryzyka i słabych stron
- Artykuł 7 ust. 4 – opracowanie wspólnych metod oceny ryzyka, zagrożeń i słabych stron.

2006/0276 (CNS)

Wniosek

DYREKYWA RADY

w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony

(Tekst mający znaczenie dla EOG)

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 308,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej, w szczególności jego art. 203,

uwzględniając wniosek Komisji[1],

uwzględniając opinię Parlamentu Europejskiego[2],

uwzględniając opinię Europejskiego Banku Centralnego[3],

a także mając na uwadze, co następuje:

(1) W czerwcu 2004 r. Rada Europejska wezwała do przygotowania ogólnej strategii ochrony infrastruktur krytycznych[4]. Odpowiadając na ten apel, w dniu 20 października 2004 r. Komisja przyjęła komunikat w sprawie ochrony infrastruktury krytycznej w walce z terroryzmem[5] zawierający propozycje usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, a także zwiększenia gotowości i zdolności reagowania na takie ataki.

(2) W dniu 17 listopada 2005 r. Komisja przyjęła zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej[6], w której opisano opcje polityczne dotyczące opracowywania tego programu oraz sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (SOZIK). Opinie uzyskane w odpowiedzi na wspomnianą zieloną księgę wyraźnie wskazują na potrzebę ustanowienia wspólnotowego zbioru przepisów regulujących ochronę infrastruktury krytycznej. Uznano potrzebę zwiększenia zdolności w zakresie ochrony infrastruktur krytycznych w Europie oraz

---

1 Dz.U. C […], […], str. […].
2 Dz.U. C […], […], str. […].
3 Dz.U. C […], […], str. […].
4 Dokument Rady 10679/2/04 REV 2
5 KOM(2004) 702.
6 KOM(2005) 576.

wsparcia działań na rzecz ograniczenia słabych stron takich infrastruktur. Podkreślono znaczenie zasady pomocniczości i dialogu zainteresowanych stron.

(3) W grudniu 2005 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wezwała Komisję do przygotowania wniosku legislacyjnego dotyczącego europejskiego programu ochrony infrastruktury krytycznej (EPOIK) i zdecydowała, że program ten powinien zakładać ochronę wszechstronną, traktując jednak przeciwdziałanie zagrożeniom terrorystycznym jako priorytet. Zgodnie z takim podejściem w procesie ochrony infrastruktury należy uwzględniać zagrożenia wywołane działalnością człowieka, zagrożenia technologiczne i klęski żywiołowe, największą uwagę poświęcając jednak zagrożeniom terrorystycznym. Jeżeli w danym sektorze infrastruktury krytycznej poziom zabezpieczenia przed określonym rodzajem poważnego zagrożenia zostanie uznany za odpowiedni, zainteresowane strony powinny skoncentrować się na tych obszarach, gdzie ochrona nadal nie jest wystarczająca.

(4) Odpowiedzialność za ochronę infrastruktury krytycznej spoczywa obecnie głównie na państwach członkowskich i właścicielach/operatorach infrastruktur krytycznych. W tym względzie nie powinno być zmian.

(5) Na terenie Wspólnoty znajduje się szereg infrastruktur krytycznych, których zakłócenie lub zniszczenie dotknęłoby co najmniej dwa państwa członkowskie lub państwo członkowskie inne niż to, w którym taka infrastruktura krytyczna jest zlokalizowana. Chodzi miedzy innymi o skutki ponadgraniczne wynikające ze współzależności między powiązanymi ze sobą infrastrukturami. Tego typu europejskie infrastruktury krytyczne należy rozpoznać i wyznaczyć za pomocą wspólnej procedury. Potrzebę zwiększenia ochrony takich infrastruktur należy ocenić na podstawie wspólnego zbioru zasad. Sprawdzonym i skutecznym środkiem rozwiązywania kwestii związanych z ponadgraniczną infrastrukturą krytyczną są dwustronne programy współpracy między państwami członkowskimi w dziedzinie ochrony infrastruktury krytycznej. EPOIK powinien opierać się na takiej właśnie współpracy.

(6) Poszczególne sektory mają własne, specyficzne doświadczenia, wiedzę i wymagania w odniesieniu do ochrony infrastruktury krytycznej, dlatego należy opracować i wdrożyć wspólnotową koncepcję ochrony infrastruktury krytycznej, biorąc pod uwagę specyfikę poszczególnych sektorów i dotychczasowe środki sektorowe, w tym środki istniejące już na poziomie UE, krajowym i regionalnym oraz obowiązujące właścicieli/operatorów infrastruktury krytycznej, transgraniczne porozumienia o wzajemnej pomocy. Wspólnotowa koncepcja musi zakładać pełne zaangażowanie sektora prywatnego z uwagi na bardzo istotny udział tego sektora w nadzorowaniu ryzyka, zarządzaniu ryzykiem, tworzeniu planów zachowania ciągłości działania i usuwaniu skutków awarii. Konieczne jest stworzenie wspólnego wykazu sektorów infrastruktury krytycznej, aby ułatwić realizację koncepcji indywidualnego traktowania poszczególnych sektorów w procesie ochrony infrastruktury krytycznej.

(7) Każdy właściciel/operator infrastruktury krytycznej powinien opracować własny plan bezpieczeństwa infrastruktury, w którym określi najważniejsze składniki infrastruktury i zaproponuje rozwiązania służące ich ochronie. Plan bezpieczeństwa infrastruktury powinien uwzględniać ocenę słabych stron, zagrożeń i ryzyka oraz inne istotne informacje dostarczone przez organy państw członkowskich.

(8) Każdy właściciel/operator europejskiej infrastruktury krytycznej powinien wyznaczyć urzędnika łącznikowego ds. bezpieczeństwa odpowiedzialnego za współpracę i komunikację z odpowiednimi krajowymi organami ds. ochrony infrastruktury krytycznej.

(9) Skuteczne rozpoznanie ryzyka, zagrożeń i słabych stron w poszczególnych sektorach wymaga komunikacji zarówno między właścicielami/operatorami europejskiej infrastruktury krytycznej a państwami członkowskimi, jak i między państwami członkowskimi a Komisją. Każde państwo członkowskie powinno gromadzić informacje dotyczące infrastruktur krytycznych zlokalizowanych na jego terytorium. Komisja powinna otrzymywać od państw członkowskich ogólne informacje na temat słabych stron, zagrożeń i ryzyka, w tym informacje na temat ewentualnych luk i współzależności międzysektorowych, które powinny stanowić podstawę opracowania szczegółowych wniosków dotyczących zwiększenia ochrony EIK, jeśli istnieje taka konieczność,.

(10) W trosce o lepszą ochronę europejskich infrastruktur krytycznych należy opracować wspólne metody rozpoznawania i klasyfikowania słabych stron, zagrożeń i ryzyka charakteryzujących poszczególne składniki infrastruktury krytycznej.

(11) Jedynie wspólne ramy prawne mogą dać gwarancję spójnego wdrażania środków służących ochronie europejskiej infrastruktury krytycznej i pozwolić na jasne określenie zakresu odpowiedzialności wszystkich uczestników procesu. Właściciele/operatorzy europejskiej infrastruktury krytycznej powinni uzyskać dostęp do najlepszych praktyk i metod w dziedzinie ochrony infrastruktury krytycznej.

(12) Skuteczna ochrona infrastruktury krytycznej wymaga komunikacji, koordynacji i współpracy na poziomie krajowym i wspólnotowym. Najlepszym sposobem osiągnięcia tego celu jest wyznaczenie w każdym państwie członkowskim punktów kontaktowych, które powinny koordynować sprawy związane z OIK na terenie tego państwa, a także odpowiadać za współpracę w tym względzie z innymi państwami członkowskimi i Komisją.

(13) Aby możliwe było prowadzenie działań służących ochronie infrastruktury krytycznej w obszarach wymagających zachowania określonego stopnia poufności, celowe jest zawarcie w niniejszej dyrektywie przepisów regulujących spójną i bezpieczną wymianę informacji. Niektóre informacje dotyczące ochrony infrastruktury krytycznej mają taki charakter, że ich ujawnienie mogłoby naruszyć interes publiczny i spowodować zagrożenie dla bezpieczeństwa publicznego. Konkretne fakty dotyczące danego składnika infrastruktury krytycznej, które można by wykorzystać do planowania i prowadzenia działań mających na celu niedopuszczalne w skutkach uszkodzenie urządzeń infrastruktury krytycznej, powinny być zastrzeżone, a dostępu do nich należy udzielać jedynie w przypadkach koniecznych, zarówno na poziomie wspólnotowym, jak i krajowym.

(14) Wymiana informacji dotyczących infrastruktury krytycznej powinna odbywać się w warunkach zaufania i bezpieczeństwa. Wymiana informacji musi opierać się na wzajemnym zaufaniu, firmy i organizacje muszą być przekonane, że dotyczące ich poufne dane są należycie chronione. Dla przedstawicieli przemysłu zachętą do wymiany informacji powinna być pewność, że korzyści płynące z dostarczenia informacji na temat infrastruktury krytycznej są w ogólnym rozrachunku społeczno-

gospodarczym większe niż koszty, jakie się z tym wiążą. Należy zatem zachęcać do wymiany informacji dotyczących ochrony infrastruktury krytycznej.

(15) Niniejsza dyrektywa jest uzupełnieniem istniejących środków sektorowych, które obowiązują na poziomie wspólnotowym i w państwach członkowskich. Tam, gdzie działają już odpowiednie mechanizmy wspólnotowe, należy nadal z nich korzystać i traktować jako wkład w ogólny proces wdrożenia niniejszej dyrektywy.

(16) Środki niezbędne do wykonania niniejszej dyrektywy powinny zostać przyjęte zgodnie z decyzją Rady 1999/468/WE z dnia 28 czerwca 1999 r. ustanawiającą warunki wykonywania uprawnień wykonawczych przyznanych Komisji[7].

(17) Państwa członkowskie same nie są w stanie osiągnąć w wystarczającym stopniu celów niniejszej dyrektywy, czyli stworzyć procedury rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz opracować wspólnej koncepcji oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur, natomiast – biorąc pod uwagę skalę takiego działania – cele te można skuteczniej osiągnąć na szczeblu wspólnotowym, dlatego Wspólnota może przyjąć środki zgodnie z zasadą pomocniczości, określoną w art. 5 Traktatu. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(18) Niniejsza dyrektywa uwzględnia prawa podstawowe i przestrzega zasad ustanowionych w szczególności w Karcie praw podstawowych Unii Europejskiej.

PRZYJMUJE NINIEJSZĄ DYREKTYWĘ:

Artykuł 1
Przedmiot

Niniejsza dyrektywa ustanawia procedury rozpoznawania i wyznaczania europejskich infrastruktur krytycznych oraz wspólne zasady oceny potrzeb w zakresie zwiększenia ochrony takich infrastruktur.

Artykuł 2
Definicje

W rozumieniu niniejszej dyrektywy:

a) „infrastruktura krytyczna” oznacza te składniki lub części infrastruktury, które mają istotne znaczenie dla utrzymania podstawowych funkcji społecznych, w tym łańcucha dostaw, zdrowia, bezpieczeństwa, ochrony i dobrobytu społeczno-gospodarczego;

b) „europejska infrastruktura krytyczna” oznacza infrastruktury krytyczne, których zakłócenie lub zniszczenie miałoby istotny negatywny wpływ na co najmniej dwa państwa członkowskie lub na jedno państwo członkowskie, w sytuacji gdy dana

[7] Dz.U. L 184 z 17.7.1999, str. 23.

infrastruktura krytyczna jest zlokalizowana w innym państwie członkowskim. Chodzi miedzy innymi o skutki wynikające ze współzależności z innymi rodzajami infrastruktury;

c) „rozmiar strat” oznacza wpływ zakłócenia lub zniszczenia danej infrastruktury w odniesieniu do:

- skutków społecznych (liczba dotkniętych mieszkańców);
- skutków ekonomicznych (wielkość strat ekonomicznych i/lub wartość utraconych towarów lub usług);
- skutków ekologicznych;
- skutków politycznych;
- skutków psychologicznych;
- konsekwencji dla zdrowia publicznego;

d) „słaba strona” oznacza cechę elementu konstrukcji, oprzyrządowania lub działania infrastruktury krytycznej, która czyni tę infrastrukturę podatną na zakłócenia lub zniszczenie i która obejmuje współzależności z innymi rodzajami infrastruktury;

e) „zagrożenie” oznacza czynnik, okoliczność lub zdarzenie, które może spowodować zakłócenie lub zniszczenie infrastruktury krytycznej lub jej elementu;

f) „ryzyko” oznacza możliwość straty, uszkodzenia lub szkody powstałej w stosunku do wartości, jaką właściciel/operator przypisał składnikowi infrastruktury, wpływ utraty takiego składnika lub jego zmiany oraz prawdopodobieństwo, że konkretne zagrożenie spowoduje zakłócenie lub zniszczenie infrastruktury w związku z jej konkretną słabą stroną;

g) „informacje dotyczące ochrony infrastruktury krytycznej” oznaczają fakty dotyczące składnika infrastruktury krytycznej, które w przypadku ujawnienia mogą zostać wykorzystane do zaplanowania lub przeprowadzenia działań zmierzających do spowodowania awarii lub wywołania niedopuszczalnego w skutkach uszkodzenia urządzeń infrastruktury krytycznej.

Artykuł 3
Rozpoznanie europejskiej infrastruktury krytycznej

1. Przekrojowe i sektorowe kryteria rozpoznawania europejskich infrastruktur krytycznych przyjmuje się zgodnie z procedurą, o której mowa w art. 11 ust. 3. Ich zmiany dokonuje się zgodnie z procedurą, o której mowa w art. 11 ust. 3.

Kryteria przekrojowe, które mają zastosowanie horyzontalne do wszystkich sektorów infrastruktury krytycznej, opracowuje się, biorąc pod uwagę rozmiar strat wynikłych

z zakłócenia lub zniszczenia danej infrastruktury. Przyjmuje się je najpóźniej [*rok po wejściu w życie niniejszej dyrektywy*].

Kryteria sektorowe opracowuje się dla sektorów priorytetowych, uwzględniając cechy charakterystyczne poszczególnych sektorów infrastruktury krytycznej i odpowiednio włączając do udziału zainteresowane strony. Kryteria takie przyjmuje się dla każdego sektora priorytetowego najpóźniej rok po wytypowaniu danego sektora jako priorytetowy.

2. Sektory priorytetowe, o których mowa w kontekście opracowania kryteriów przewidzianych w ust. 1, wyznacza co roku Komisja spośród wymienionych w załączniku 1.

Do załącznika I wprowadza się zmiany zgodnie z procedurą, o której w art. 11 ust. 3, i w stopniu, który nie powoduje rozszerzenia zakresu niniejszej dyrektywy.

3. Każde państwo członkowskie rozpoznaje infrastruktury krytyczne zlokalizowane na swoim terytorium – a także infrastruktury krytyczne, które mogą mieć wpływ na to państwo chociaż są zlokalizowane poza granicami jego terytorium – które spełniają kryteria przyjęte na podstawie ust. 1 i 2.

Każde państwo członkowskie zgłasza Komisji tak określone infrastruktury najpóźniej rok od przyjęcia odpowiednich kryteriów, a potem na bieżąco.

Artykuł 4
Wyznaczanie europejskiej infrastruktury krytycznej

1. Na podstawie zgłoszeń dokonanych zgodnie z art. 3 ust. 3 akapit drugi i innych dostępnych informacji Komisja przedstawia wykaz infrastruktur krytycznych wyznaczonych jako europejskie infrastruktury krytyczne.

2. Wykaz infrastruktur krytycznych wyznaczonych jako europejskie infrastruktury krytyczne przyjmuje się zgodnie z procedurą, o której mowa w art. 11 ust. 3.

Zmiany do wykazu wprowadza się zgodnie z procedurą, o której mowa w art. 11 ust. 3.

Artykuł 5
Plany zabezpieczenia infrastruktury

1. Każde państwo członkowskie nakłada na właścicieli/operatorów wszystkich europejskich infrastruktur krytycznych znajdujących się na jego terytorium obowiązek stworzenia i uaktualniania planu bezpieczeństwa infrastruktury oraz dokonywania przeglądu takiego planu co najmniej raz na dwa lata.

2. W planie bezpieczeństwa infrastruktury należy określić składniki europejskiej infrastruktury krytycznej i podać odpowiednie rozwiązania gwarantujące ich ochronę zgodnie z załącznikiem II. Wymogi sektorowe dotyczące planu bezpieczeństwa infrastruktury z uwzględnieniem istniejących środków wspólnotowych przyjmuje się zgodnie z procedurą, o której mowa w art. 11 ust. 3.

Postępując zgodnie z procedurą, o której mowa w art. 11 ust. 2, Komisja może uznać, że przestrzeganie przepisów obowiązujących w określonych sektorach wymienionych w załączniku I jest jednoznaczne ze spełnieniem wymogu stworzenia i uaktualniania planu bezpieczeństwa infrastruktury.

3. Nie później niż rok od daty wyznaczenia danej infrastruktury krytycznej jako europejska infrastruktura krytyczna jej właściciel/operator przedkłada odpowiedniemu organowi państwa członkowskiego plan bezpieczeństwa infrastruktury.

Jeśli przyjęto wymogi sektorowe dotyczące planu bezpieczeństwa infrastruktury w oparciu o przepisy ust. 2, plan taki należy przedłożyć odpowiedniemu organowi państwa członkowskiego nie później niż rok od daty przyjęcia takich wymogów sektorowych.

4. Każde państwo członkowskie tworzy system zapewniający właściwy i regularny nadzór nad planami bezpieczeństwa infrastruktury i sposobami ich wdrażania, oparty na ocenach ryzyka i zagrożeń prowadzonych zgodnie z art. 7 ust. 1.

5. Wykonanie przepisów dyrektywy 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów uznaje się za równoznaczne ze spełnieniem wymogu opracowania planu bezpieczeństwa infrastruktury.

Artykuł 6
Urzędnik łącznikowy ds. bezpieczeństwa

1. Każde państwo członkowskie nakłada na właścicieli/operatorów europejskich infrastruktur krytycznych zlokalizowanych na swoim terytorium obowiązek wyznaczenia urzędnika łącznikowego ds. bezpieczeństwa działającego jako skrzynka kontaktowa w sprawach bezpieczeństwa dla właścicieli/operatorów infrastruktury i właściwych organów ds. ochrony infrastruktury krytycznej w państwach członkowskich. Urzędnika łącznikowego ds. bezpieczeństwa wyznacza się najpóźniej rok od daty wyznaczenia danej infrastruktury krytycznej jako europejska infrastruktura krytyczna.

2. Każde państwo członkowskie przekazuje urzędnikowi łącznikowemu ds. bezpieczeństwa istotne informacje dotyczące rozpoznanych zagrożeń i ryzyka dla danej europejskiej infrastruktury krytycznej.

Artykuł 7
Sprawozdawczość

1. Każde państwo członkowskie dokonuje oceny ryzyka i zagrożeń w odniesieniu do EIK zlokalizowanej na swoim terytorium nie później niż rok od daty wyznaczenia danej infrastruktury krytycznej jako EIK.

2. Każde państwo członkowskie przekazuje Komisji skrócone zestawienie słabych stron, typów zagrożeń i ryzyka stwierdzonych w każdym z sektorów wymienionych

w załączniku I nie później niż 18 miesięcy od daty przyjęcia wykazu przewidzianego w art. 4 ust. 2, a potem na bieżąco.

Wspólny wzór takich sprawozdań opracowuje się zgodnie z procedurą, o której mowa w art. 11 ust. 3

3. Komisja ocenia na zasadzie indywidualnej, czy w poszczególnych sektorach europejskiej infrastruktury krytycznej wymagane jest wprowadzenie konkretnych środków zabezpieczających.

4. Wspólne metody oceny słabych stron, zagrożeń i ryzyka w odniesieniu do europejskich infrastruktur krytycznych, opracowuje się według sektorów, zgodnie z procedurą, o której mowa w art. 11 ust. 3.

Artykuł 8
Wsparcie dla właścicieli/operatorów EIK

Komisja udziela właścicielom/operatorom wyznaczonych europejskich infrastruktur krytycznych wsparcia polegającego na udostępnieniu im najlepszych praktyk i metod w zakresie ochrony infrastruktury krytycznej.

Artykuł 9
Punkty kontaktowe ds. OIK

1. Każde państwo członkowskie wyznacza punkty kontaktowe ds. ochrony infrastruktury krytycznej.

2. Punkt kontaktowy koordynuje sprawy związane z ochroną infrastruktury krytycznej w obrębie danego państwa członkowskiego, a także odpowiada za współpracę w tym względzie z innymi państwami członkowskimi i Komisją.

Artykuł 10
Poufność i wymiana informacji dotyczących OIK

1. Stosując niniejszą dyrektywę, Komisja podejmuje odpowiednie środki zgodnie z decyzją 2001/844/WE, EWWiS, Euratom, aby chronić informacje, których dotyczy wymóg zachowania poufności, a do których ma dostęp lub które zostały jej przekazane przez państwa członkowskie. Państwa członkowskie podejmują równoważne działania zgodnie z odnośnym ustawodawstwem krajowym. Należy w odpowiedni sposób uwzględnić wagę potencjalnego uchybienia w tej dziedzinie dla istotnych interesów Wspólnoty czy też jednego lub większej liczby państw członkowskich.

2. Każda osoba, która na mocy niniejszej dyrektywy zajmuje się przetwarzaniem informacji w imieniu państwa członkowskiego, podlega odpowiedniej kontroli tego państwa pod kątem przestrzegania zasad ochrony danych.

3. Państwa członkowskie dbają o to, by informacje dotyczące ochrony infrastruktury krytycznej przekazywane państwom członkowskim lub Komisji nie były wykorzystywane do celów innych niż ochrona infrastruktur krytycznych.

Artykuł 11
Komitet

1. Komisję wspomaga komitet, w skład którego wchodzi po jednym przedstawicielu każdego punktu kontaktowego ds. OIK.

2. W przypadku odesłania do niniejszego ustępu, zastosowanie mają art. 3 i 7 decyzji Rady 1999/468/WE, z uwzględnieniem przepisów art. 8 tejże decyzji.

3. W przypadku odesłania do niniejszego ustępu, zastosowanie mają art. 5 i 7 decyzji Rady 1999/468/WE, z uwzględnieniem przepisów art. 8 tejże decyzji.

   Okres przewidziany w art. 5 ust. 6 decyzji 1999/468/WE ustala się na jeden miesiąc.

4. Komitet przyjmuje swój regulamin wewnętrzny.

Artykuł 12
Wprowadzenie w życie

1. Państwa członkowskie wprowadzą w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy najpóźniej do dnia 31 grudnia 2007 r. Państwa członkowskie niezwłocznie przekazują Komisji tekst tych przepisów oraz tabelę korelacji między tymi przepisami a niniejszą dyrektywą.

   Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposób dokonania takiego odniesienia ustalany jest przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji tekst głównych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 13
Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 14
Adresaci

Niniejsza dyrektywa skierowana jest do wszystkich państw członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady

ZAŁĄCZNIK I

WYKAZ SEKTORÓW INFRASTRUKTURY KRYTYCZNEJ

Sektor		Podsektor	
I	Energia	1	Produkcja, rafinacja, przetwarzanie, magazynowanie i rozprowadzanie rurociągami ropy naftowej i gazu
		2	Wytwarzanie i przesyłanie energii elektrycznej
II	Przemysł jądrowy	3	Produkcja i magazynowanie/przetwarzanie substancji jądrowych
III	Technologie informacyjno-komunikacyjne (ICT)	4	Ochrona systemów i sieci informatycznych
		5	Systemy oprzyrządowania, automatyzacji i kontroli (SCADA itp.)
		6	Internet
		7	Świadczenie usług telekomunikacji stacjonarnej
		8	Świadczenie usług telekomunikacji komórkowej
		9	Radiokomunikacja i nawigacja
		10	Komunikacja satelitarna
		11	Nadawanie radiowo-telewizyjne
IV	Woda	12	Dostawy wody pitnej
		13	Kontrola jakości wody
		14	Monitorowanie i ilościowa kontrola zasobów wodnych
V	Żywność	15	Dostawy żywności oraz zapewnienie bezpieczeństwa żywności i bezpieczeństwa dostaw
VI	Zdrowie	16	Opieka medyczna i szpitalna
		17	Lekarstwa, surowice, szczepionki i środki farmaceutyczne
		18	Laboratoria i czynniki biologiczne
VII	Sektor finansowy	19	Infrastruktury i systemy płatnościowe i rozrachunkowo-rozliczeniowe
		20	Rynki regulowane
VIII	Transport	21	Transport drogowy
		22	Transport kolejowy
		23	Transport lotniczy
		24	Wodny transport śródlądowy
		25	Żegluga oceaniczna i morska żegluga bliskiego zasięgu
IX	Przemysł chemiczny:	26	Produkcja i magazynowanie/przetwarzanie substancji chemicznych
		27	Rurociągi do transportu towarów niebezpiecznych (substancji chemicznych)
X	Przestrzeń kosmiczna	28	Przestrzeń kosmiczna
XI	Infrastruktura badawcza	29	Infrastruktura badawcza

ZAŁĄCZNIK II

PLAN BEZPIECZNEJ OBSŁUGI (PBI)

W PBI określa się składniki infrastruktur krytycznych i opracowuje odpowiednie rozwiązania służące ich ochronie. PBI obejmuje co najmniej:

– rozpoznanie ważnych składników infrastruktury;

– analizę ryzyka opartą na scenariuszach poważnych zagrożeń, analizę słabych stron poszczególnych składników infrastruktury i analizę potencjalnych skutków.

– rozpoznanie, selekcję i ustalenie hierarchii ważności środków przeciwdziałania i procedur, z podziałem na:

- **Stałe środki bezpieczeństwa**, określające niezbędne inwestycje i środki w dziedzinie bezpieczeństwa, które nie mogą zostać zainstalowane przez właściciela/operatora w krótkim czasie. W tej części planu znajdą się informacje dotyczące środków ogólnych; środków technicznych (w tym instalacja urządzeń wykrywających, kontrola dostępu, środki zabezpieczające i zapobiegawcze); środki organizacyjne (w tym procedury sygnalizowania zagrożeń i zarządzania kryzysowego); środki kontrolno-weryfikacyjne; komunikacja; podnoszenie świadomości społecznej i szkolenia oraz bezpieczeństwo systemów informacyjnych.

- **Doraźne środki bezpieczeństwa**, które uruchamia się w zależności od zmieniającego się poziomu ryzyka i zagrożenia.

OCENA SKUTKÓW FINANSOWYCH REGULACJI

Obszar(y) polityki: Wymiar sprawiedliwości i sprawy wewnętrzne

Działanie: Ochrona infrastruktury krytycznej

TYTUŁ DZIAŁANIA: Dyrektywa w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony

1. 1. POZYCJA(E) W BUDŻECIE + TREŚĆ

Nie dot.

2. OGÓLNE DANE LICZBOWE

2.1. Całkowite środki przydzielone na działanie (część B): zobowiązanie w mln EUR

Nie dot.

2.2. Czas trwania działania:

od 2006 r.

2.3. Całkowity wieloletni preliminarz wydatków:

a) Harmonogram przydziału środków na zobowiązania/środków na płatności (interwencja finansowa) (*patrz pkt 6.1.1*)

mln EUR (*do trzech miejsc po przecinku*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Razem
Zobowiązania	-	-	-	-	-	-	-
Płatności	-	-	-	-	-	-	-

b) Pomoc techniczna i administracyjna oraz wydatki pomocnicze (*zob. pkt 6.1.2*)

Zobowiązania	-	-	-	-	-	-	-
Płatności	-	-	-	-	-	-	-

Razem a+b	-	-	-	-	-	-	-
Zobowiązania	-	-	-	-	-	-	-
Płatności	-	-	-	-	-	-	-

c) Całkowite skutki finansowe wydatków na zasoby ludzkie i pozostałych wydatków administracyjnych*(patrz pkt 7.2 i 7.3)*

Zobowiązania/płatności	1,280	1,280	1,280	1,280	1,280	1,280	1,280

OGÓŁEM a+b+c	1,280	1,280	1,280	1,280	1,280	1,280	1,280
Zobowiązania	1,280	1,280	1,280	1,280	1,280	1,280	1,280
Płatności	1,280	1,280	1,280	1,280	1,280	1,280	1,280

2.4. Zgodność z programowaniem finansowym i perspektywą finansową

Niniejsza dyrektywa jest zgodna z programem zapobiegania, gotowości i zarządzania skutkami terroryzmu i innych zagrożeń dla bezpieczeństwa na lata 2007–2013.

2.5. Wpływ finansowy na dochody:

Niedawno przyjęty program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innych zagrożeń dla bezpieczeństwa" w okresie 2007–2013 (z budżetem 137,5 mln EUR) będący częścią szerszego programu „Bezpieczeństwo i ochrona swobód", przyczyni się do wdrożenia EPOIK, wpływając na wzmocnienie ochrony osób oraz tych zasobów materialnych, usług, sprzętu informatycznego, sieci i składników infrastruktury, których zakłócenie lub zniszczenie miałoby poważny wpływ na podstawowe funkcje społeczne. Program ma ograniczony zakres, gdyż nie obejmuje inwestycji związanych ze sprzętem i wyposażeniem. Program ten nie odnosi się do spraw, które są objęte zakresem działania innych instrumentów finansowych, szczególnie instrumentu szybkiego reagowania w przypadku poważnych sytuacji kryzysowych.

W odniesieniu do zapobiegania atakom terrorystycznym i zapewnianie gotowości, celem programu jest:

a) stymulowanie, promowanie i wspieranie ocen ryzyka i zagrożenia infrastruktury krytycznej, w tym ocen na miejscu dla rozpoznania zagrożeń i słabych stron oraz potrzeb w zakresie zwiększenia poziomu ochrony;

b) promowanie i wspieranie wspólnych środków operacyjnych służących wzmocnieniu ochrony łańcuchów dostaw transgranicznych, pod warunkiem przestrzegania reguł konkurencji na rynku wewnętrznym;

c) promowanie i wspieranie procesu tworzenia minimalnych norm bezpieczeństwa, najlepszych praktyk w zakresie wymiany informacji, narzędzi oceny ryzyka, metod porównywania infrastruktur w różnych sektorach i ustalania ich ważności, analizy słabych stron i współzależności infrastruktur krytycznych.

d) promowanie i wspieranie koordynacji i współpracy w zakresie ochrony infrastruktury krytycznej w skali całej Wspólnoty, a w razie potrzeby formułowanie wniosków dotyczących minimalnych środków zabezpieczających i wspólnych wytycznych.

W odniesieniu do zarządzania skutkami ataków terrorystycznych celem programu jest:

a) stymulowanie, promowanie i wspieranie wymiany know-how, doświadczeń i technologii;

b) stymulowanie, promowanie i wspieranie procesu opracowywania odpowiednich metod i planów awaryjnych;

c) zapewnienie przekazywania w czasie rzeczywistym konkretnej wiedzy fachowej w dziedzinie bezpieczeństwa w ramach ogólnych mechanizmów zarządzania kryzysowego, szybkiego ostrzegania i ochrony ludności.

Wniosek nie ma zatem wpływu finansowego na dochody.

3. INFORMACJE BUDŻETOWE

Rodzaj wydatków		**Nowe**	**Wkład EFTA**	**Wkład krajów ubiegających się o członkostwo**	**Dział w perspektywie finansowej**
nieobowiązkowe	Niezróżnicowane	Nie dot.	Nie dot.	Nie dot.	Brak nie dot.

4. PODSTAWA PRAWNA

Podstawą prawną wniosku jest art. 308 Traktatu ustanawiającego Wspólnotę Europejską.

5. OPIS I UZASADNIENIE

5.1. 5.1. Potrzeba udziału Wspólnoty

5.1.1. Wyznaczone cele

Środek prawny w postaci dyrektywy najlepiej nadaje się do stworzenia wspólnego zbioru zasad regulujących EPOIK, gdyż państwa członkowskie charakteryzują się różnym podejściem do zagadnienia ochrony infrastruktury krytycznej oraz mają różne tradycje prawne w tej materii. Wskazując główne kierunki działań i pozwalając państwom członkowskim przyjąć rozwiązania, które najlepiej odpowiadają ich potrzebom, można w pełni osiągnąć cele EPOIK, wykorzystując przy tym dotychczasowe osiągnięcia.

5.1.2. Środki podjęte w związku z oceną ex ante

W kwestiach związanych z opracowaniem EPOIK zasięgnięto opinii wszystkich zainteresowanych stron. Płaszczyzną konsultacji były:

- Zielona księga w sprawie EPOIK, przyjęta 17 listopada 2005 r., z okresem konsultacji do 15 stycznia 2006 r. Swoje opinie zgłosiło 22 państwa członkowskie. Uwagi w sprawie zielonej księgi nadesłało także około 100

przedstawicieli sektora prywatnego. W opiniach tych wyrażano przeważnie poparcie dla idei stworzenia EPOIK.

- Trzy seminaria poświęcone ochronie infrastruktury krytycznej, których gospodarzem była Komisja (w czerwcu 2005 r., wrześniu 2005 r. i marcu 2006 r.). We wszystkich trzech seminariach brali udział przedstawiciele państw członkowskich. Osoby reprezentujące sektor prywatny zaproszono na seminaria we wrześniu 2005 r. i marcu 2006 r.

- Nieformalne spotkania punktów kontaktowych ds. OIK. Komisja zorganizowała dwa spotkania z udziałem przedstawicieli punktów kontaktowych ds. OIK z państw członkowskich (grudzień 2005 r. i luty 2006 r.).

- Nieformalne spotkania z przedstawicielami sektora prywatnego. Zorganizowano liczne nieformalne spotkania z przedstawicielami konkretnych przedsiębiorstw, jak również z przedstawicielami stowarzyszeń branżowych.

- W samej Komisji prace nad opracowaniem EPOIK postępowały dzięki regularnym spotkaniom podgrupy ds. ochrony infrastruktury krytycznej wyłonionej z międzydepartamentalnej grupy ds. wewnętrznych aspektów terroryzmu.

5.2. Planowane działanie i uzgodnienia dotyczące interwencji budżetu

Wpływ proponowanej regulacji na budżet przedstawiono w załączonej do niniejszego wniosku ocenie skutków finansowych.

5.3. Metody wykonywania

Ponieważ chodzi o dyrektywę, nie jest wymagane podanie metody wykonania budżetu.

6. WPŁYW FINANSOWY

6.1. Całkowity wpływ finansowy na część B - (podczas całego okresu programowania)

6.1.1. Interwencja finansowa

Nie dot.

6.1.2. Pomoc techniczna i administracyjna, wydatki pomocnicze oraz wydatki IT (środki na zobowiązania)

Nie dot.

6.2. Kalkulacja kosztów według działań przewidzianych w części B (podczas całego okresu objętego programowaniem)

Nie dot.

7. 7. WPŁYW NA WYDATKI PERSONALNE I ADMINISTRACYJNE

7.1. Wpływ na zasoby ludzkie

Rodzaj stanowiska		Personel, który przypisany zostanie do zarządzania działaniem przy użyciu istniejących zasobów		Razem	Opis zadań związanych z działaniem
		Liczba stanowisk stałych	Liczba stanowisk czasowych		
Urzędnicy zatrudnieni na stałe pracownicy zatrudnieni na czas określony	A B C	8 A 1 B	1 C	10	Gromadzenie i przetwarzanie informacji, Przygotowanie posiedzeń komitetu
Pozostałe zasoby ludzkie					
Razem		9	1	10	

Zapotrzebowanie w zakresie zasobów ludzkich i administracyjnych zostanie pokryte z przydziału przyznanego zarządzającej DG w ramach corocznej procedury przydziału środków.

7.2. Całkowity wpływ finansowy na zasoby ludzkie

Rodzaj zasobów ludzkich	Kwota (EUR)	Metoda obliczania
Urzędnicy Pracownicy czasowi	1.080.000 48.000	(108.000x10=1.080.000 4.000 x 12 = 48.000
Pozostałe zasoby ludzkie (określić pozycję w budżecie)		
Razem	1.128.000	

Podane kwoty odpowiadają wydatkom całkowitym w okresie 12 miesięcy.

7.3. Inne wydatki administracyjne wynikające z działania

Pozycja w budżecie (numer i treść)	Kwota (EUR)	Metoda obliczania
Przydział ogółem (tytuł A7)		
A0701 - Podróże służbowe	24.000	2000x12 mies.=24.000
A07030 - Spotkania	-	-
A07031 – Komitety obowiązkowe	128.000	32.000 x 4 spotkania rocznie=128.000
A07032 – Komitety nieobowiązkowe	-	-
A07040 - Konferencje	-	-
A0705 - Badania i konsultacje	-	-
Inne wydatki (określić)		
Systemy informatyczne (A-5001/A-4300)	-	-
Inne wydatki – Część A (określić)		

Razem	152.000	

Podane kwoty odpowiadają wydatkom całkowitym w okresie 12 miesięcy.

Określić rodzaj komitetu i grupę, do której należy.

I.	Ogółem rocznie (7.2 + 7.3)	1.280.000
II.	Czas trwania działania	Ciągły
III.	Koszt całkowity działania (I x II)	

8. DZIAŁANIA NASTĘPCZE I OCENA

8.1. Uzgodnienia związane z działaniami następczymi

Nie dot.

8.2. Uzgodnienia dotyczące planowanej oceny i harmonogram oceny

Nie dot.

9. ŚRODKI ZWALCZANIA NADUŻYĆ FINANSOWYCH

Nie dot.