Wtorek, 7 czerwca 2005 r.

P6_TA(2005)0221

Ochrona infrastruktury o kluczowym znaczeniu w ramach walki z terroryzmem

Zalecenie Parlamentu Europejskiego dla Rady Europejskiej i Rady w sprawie ochrony infrastruktury o kluczowym znaczeniu w ramach walki z terroryzmem (2005/2044(INI))

Parlament Europejski,

— uwzględniając projekt zalecenia dla Rady, złożonego przez Stavrosa Lambrinidisa w imieniu grupy politycznej PSE w sprawie ochrony infrastruktur o kluczowym znaczeniu w ramach walki z terroryzmem (B6-0085/2005),

— uwzględniając Traktat Konstytucyjny, a w szczególności jego art. III-284 dotyczący obrony cywilnej i art. I-43, który przewiduje, że „Unia i jej Państwa Członkowskie działają wspólnie w duchu solidarności, jeżeli jakiekolwiek Państwo Członkowskie stanie się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej bądź katastrofy spowodowanej przez człowieka",

— uwzględniając Deklarację solidarności przeciwko terroryzmowi przyjętą przez głowy państw i rządów dnia 25 marca 2004 r.,

— uwzględniając tzw. program haski ([1]) przyjęty w dniu 5 listopada 2004 r., według którego „…skuteczne zarządzanie ponadgranicznymi sytuacjami kryzysowymi na obszarze UE wymaga nie tylko wzmocnienia bieżących działań dotyczących obrony cywilnej i niezbędnej infrastruktury, lecz także skutecznego zwrócenia uwagi na porządek publiczny i aspekty bezpieczeństwa w takich sytuacjach kryzysowych… Dlatego Rada Europejska wzywa Radę i Komisję do utworzenia…… zintegrowanego mechanizmu zarządzania kryzysowego…. który powinien wejść w życie do dnia 1 lipca 2006 r. Mechanizm ten powinien dotyczyć przynajmniej następujących kwestii: dodatkowej oceny możliwości Państw Członkowskich, gromadzenia zapasów, szkoleń, wspólnych ćwiczeń i planów operacyjnych dla cywilnego zarządzania kryzysowego",

— uwzględniając komunikaty Komisji:

a) do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie zwiększania potencjału obrony cywilnej Unii Europejskiej (COM(2004)0200), który ocenia dotychczas osiągnięte wyniki, słabe punkty i ewentualną poprawę potencjału obrony cywilnej Unii Europejskiej, zwłaszcza jako pierwszego instrumentu interwencji kryzysowej opartego na zasadzie dobrowolności,

b) do Rady i Parlamentu Europejskiego w sprawie zapobiegania, gotowości i reagowania na ataki terrorystyczne (COM(2004)0698), który podkreśla potrzebę zintegrowanego podejścia Wspólnoty, które powinno m.in. koncentrować się na właściwej komunikacji władz ze społeczeństwem w przypadku kryzysu, roli EUROPOL-u w tworzeniu mechanizmu ostrzegania organów ścigania w celu odpowiedniego postępowania w przypadkach terroryzmu i ustanowieniu Europejskiego Programu Ochrony Infrastruktury Strategicznej (EPOIS), badaniach w dziedzinie bezpieczeństwa i angażowaniu w sposób planowy odpowiednich części sektora prywatnego,

c) do Rady i Parlamentu Europejskiego w sprawie gotowości i radzenia sobie z konsekwencjami w walce z terroryzmem (COM(2004)0701), który proponuje konsolidację systemów alarmowych zarządzanych przez Komisję w ramach bezpiecznego ogólnego systemu szybkiego ostrzegania (ARGUS) połączonego z Centralnym Centrum Kryzysowym, które gromadziłoby przedstawicieli odpowiednich służb Komisji i zapewniło stały kontakt pomiędzy Państwami Członkowskimi i instytucjami europejskimi,

d) do Rady i Parlamentu Europejskiego w sprawie ochrony infrastruktury strategicznej w walce z terroryzmem (COM(2004)0702), który proponuje ustanowienie EPOIS we współpracy z Państwami Członkowskimi oraz odpowiednimi częściami sektora prywatnego w celu identyfikacji potencjalnych niedociągnięć i środków naprawczych (prawnych lub innych), które należy zastosować,

([1]) Zaktualizowany 17 grudnia 2004 r. w kwestii walki z terroryzmem.

— uwzględniając swoją rezolucję z dnia 4 września 2003 r. w sprawie skutków letniej fali upałów ([1]), w której apelował on o utworzenie Europejskich Sił Obrony Cywilnej,

— uwzględniając stosowne podstawy prawne ustanowione w Traktatach, które uprawniają Wspólnotę i Unię do określania i wdrażania polityk wspierających działania Państw Członkowskich w zakresie ochrony zdrowia i bezpieczeństwa obywateli europejskich,

— uwzględniając art. 114 ust. 3 oraz art. 94 Regulaminu,

— uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A6-0161/2005),

A. świadomy faktu, iż obywatele Europy wciąż potrzebują ochrony przed ryzykiem związanym z atakami terrorystycznymi (takimi jak ataki nuklearne, radiologiczne, chemiczne i biologiczne, ataki w miejscach publicznych, itp.), lecz również z klęskami żywiołowymi (takimi jak trzęsienia ziemi, powodzie, pożary, pożary lasów), katastrofami technologicznymi (takimi jak katastrofa w Seveso, katastrofy morskie, wypadki transportowe), jak również kryzysami zdrowotnymi lub innymi (np. pandemiami), w kontekście zintegrowanej strategii europejskiej, uwzględniając, że takie wydarzenia nie tylko powoduja poważne skutki ponadgraniczne na poziomie europejskim, lecz również powodują konieczność wykazania przez Państwa Członkowskie wzajemnej solidarności oraz istnienia konsekwentnego i interoperacyjnego systemu reagowania,

B. stwierdzając, że efektywna strategia powinna koncentrować się zarówno na gotowości (ocena ryzyka i zagrożenia dla strategicznej infrastruktury, środki podwyższonego bezpieczeństwa, promowanie wspólnych norm bezpieczeństwa i wymiany fachowej wiedzy, promowanie koordynacji i współpracy na skalę UE), jak i radzeniu sobie ze skutkami ataków i katastrof (wymiana wiedzy, umiejętności i doświadczenia, opracowanie scenariuszy i ćwiczenia szkoleniowe oraz ustanowienie stosownych mechanizmów zarządzania kryzysami, szybkiego ostrzegania i obrony cywilnej),

C. przekonany, że zwłaszcza w przypadku ataków terrorystycznych, w których sprawcy obeszli systemy zabezpieczeń i odstraszania, jedynie dobrze zorganizowany i skuteczny system reagowania może zagwarantować szybki powrót do normalności; że wyłącznie dzięki podnoszeniu specjalistycznych umiejętności, ścisłej współpracy, gromadzeniu środków, zagwarantowaniu oceny ryzyka, informacjom, szkoleniom, komunikacji, analizie zapobiegawczej i analizie skutków katastrof można zapewnić natychmiastowe przywrócenie normalności i że wreszcie Państwa Członkowskie i UE, poprzez zwiększanie środków i udzianie niezbędnej pomocy ofiarom, mogą lepiej chronić swych obywateli w przypadku wystąpienia w UE lub poza jej terytorium katastrof, których skutki pośrednio lub bezpośrednio dotknęłyby obywateli UE,

D. stwierdzając, że w strategicznej infrastrukturze w UE powstają silne powiązania i współzależności, przez co staje się ona bardziej podatna na zakłócenia lub zniszczenie,

E. uznając, że ochrona infrastruktur o kluczowym znaczeniu wymaga konsekwentnego i opartego na współpracy partnerstwa właścicieli i operatorów tejże infrastruktury oraz władz Państw Członkowskich; odnotowując, że analizowanie i zarządzanie ryzykiem w przypadku każdej infrastruktury musi opierać się na surowych, określonych przez UE, standardach i procedurach; odnotowując, że odpowiedzialność za zarządzanie ryzykiem w obiektach, w ramach łańcucha dostaw, technologii informacyjnych i sieci komunikacyjnych ostatecznie spoczywa na właścicielach i operatorach, na których spoczywa obowiązek codziennego kierowania tymi infrastrukturami; odnotowując jednakże, iż UE i Państwa Członkowskie powinny udzielać pomocy sektorowi przemysłowemu w wykonywaniu jego obowiązków, szkolić, wspierać i kontrolować na wszystkich szczeblach organów władzy publicznej, w tym poprzez bodźce finansowe i inne, jeżeli i wtedy, gdy zostanie to uznane za stosowne; odnotowując, w tym zakresie, że operatorzy powinni mieć możliwość przekazywania aktualnych informacji władzom, a te ostatnie powinny wziąć odpowiedzialność za analizowanie informacji oraz opracowanie odpowiednich rozwiązań zapewniających bezpieczeństwo wspólnie z operatorami; mając na uwadze, że istotne jest zapewnienie podstawowego prawa do ochrony danych na szczeblu europejskim i krajowym w każdym poszczególnym przypadku powiązanym z tą działalnością,

([1]) Dz.U. C 76 E z 25.3.2004, str. 382.

F. przekonany, że wobec coraz większej złożoności zagrożeń należy rozbudować komputerowe systemy zabezpieczeń we współpracy z właściwymi organami na szczeblu krajowym i europejskim (np. ENISA) i wykorzystując najwyższej klasy technologie informatyczne,

1. występuje do Rady Europejskiej i do Rady z następującymi zaleceniami:

a) pełna realizacja projektu Rady Europejskiej zakładającego utworzenie „zintegrowanego systemu zarządzania kryzysami UE" jako zasadniczego elementu zacieśniania więzi pomiędzy obywatelami i instytucjami UE i wzmacniania wzajemnej zależności i solidarności Państw Członkowskich;

b) zapewnienie, aby zintegrowana strategia europejska uwzględniała przede wszystkim potencjalne zagrożenia dla strategicznej infrastruktury, w tym urządzeń informatycznych, której unieruchomienie lub zniszczenie oznaczałoby poważne konsekwencje dla zdrowia, bezpieczeństwa lub sytuacji ekonomicznej obywateli oraz opracowanie jednolitego mechanizmu wspólnotowego tak aby, dzięki wspólnym normom oraz organizacjom i osobom odpowiedzialnym za bezpieczeństwo, Państwa Członkowskie i podmioty eksploatujące były w stanie zidentyfikować infrastrukturę o kluczowym znaczeniu, dokonać analizy jej słabych punktów i współzależności oraz ponadgranicznych skutków ewentualnych kryzysów, a także dokonać właściwej oceny istotnych zagrożeń, jak również opracować rozwiązania mające na celu ochronę i przygotowanie takiej infrastruktury na wszelkie niebezpieczeństwa oraz zapewnić odpowiednią reakcję w przypadku zamachu lub katastrofy;

c) ustanowienie, na wniosek Komisji i za zgodą Parlamentu, Europejskiego Programu Ochrony Infrastruktury Strategicznej (EPOIS), który wymagałby finansowania ze strony Państw Członkowskich oraz/lub właścicieli i operatorów, w oparciu o zachęty finansowe lub inne, jeżeli i wtedy, gdy jest to stosowne; uczestniczące w nim Państwa Członkowskie powinny zapewnić pełną współpracę, łącznie ze współpracą publiczno-prywatną oraz udostępnić wszelkie informacje, zasoby ludzkie i logistyczne potrzebne dla pomyślnego ukończenia poszczególnych faz projektu, aby spełnić w ten sposób wymogi proporcjonalności i pomocniczości, przede wszystkim w odniesieniu do praw obywatelskich, ochrony danych i wymogów bezpieczeństwa;

d) uwzględnienie faktu, iż EPOIS powinien być uznawany przez organy ścigania Państw Członkowskich oraz organy odpowiedzialne za krajowe mechanizmy obrony cywilnej za element uzupełniający krajowe planowanie i podnoszenie świadomości; iż powodzenie EPOIS należy oceniać w sposób niezależny i zgodnie z określonymi normami; oraz że, na wniosek Komisji, Rada powinna ustanowić EPOIS według określonego i realnego kalendarza stopniowej realizacji ustalonych i wyraźnie sprecyzowanych etapów i celów; oraz uznanie, że sukces Europejskiej Sieci Informacyjnej Wczesnego Ostrzegania o Zagrożeniach Infrastruktury Strategicznej wymaga, aby sieć ta wspierała stymulację wymiany informacji na temat wspólnych zagrożeń i wzajemnej wrażliwości oraz opracowanie stosownych środków i strategii zmniejszających ryzyko w celu ochrony infrastruktury o kluczowym znaczeniu;

e) uznanie faktu, iż:

— należy utworzyć, we współpracy z Europejskim Inspektorem Ochrony Danych, europejski system analizy ryzyka w celu zapewnienia interoperacyjności, mając na uwadze wymogi ochrony danych na szczeblu europejskim i krajowym;

— należy zapewnić koordynację między wszelkimi odpowiednimi organami na szczeblu krajowym, europejskim i międzynarodowym, prowadzącymi wymianę informacji, przy zaangażowaniu urzędów ochrony danych na poszczególnych szczeblach;

— istotne informacje powinny być przetwarzane, niezależnie od tego, z jakiego źródła pochodzą (wywiad wojskowy lub cywilny, współpraca policyjna), w sposób staranny, rzetelny i w razie potrzeby z zachowaniem zasady poufności; należy zawsze zapewnić stosowną kontrolę Parlamentu, zawierając w tym celu specjalne porozumienie międzyinstytucjonalne, jeżeli zagrożenie dotyczy kwestii europejskiego bezpieczeństwa wewnętrznego;

— konieczne jest stworzenie w obrębie Komisji europejskiego systemu wczesnego ostrzegania kryzysowego, by połączyć istniejące europejskie, krajowe i międzynarodowe specjalistyczne systemy wczesnego ostrzegania w stanach zagrożenia, tak aby umożliwić efektywne udostępnianie wszystkich istotnych informacji, które mogą wymagać działania na szczeblu europejskim, przez sieć centralną (ARGUS);

— wskazane jest nawiązanie współpracy z Europejskim Komitetem Normalizacyjnym (CEN), jeżeli nie istnieją normy sektorowe lub nie zostały jeszcze ustanowione normy międzynarodowe;

f) zapewnienie, iż EPOIS:

— znajduje się pod stałą kontrolą parlamentarną na szczeblu europejskim i krajowym,

— stanowi zasadniczy element przyszłych zmian na poziomie kontynentalnym i światowym ([1]);

g) poprawa funkcjonowania Europejskiego Funduszu Solidarności (dla interwencji w Unii) i ECHO (dla interwencji zewnętrznych) jako działanie uzupełniające;

h) podjęcie propozycji zawartej w wyżej wymienionej rezolucji, która wzywa do utworzenia Europejskich Sił Obrony Cywilnej, które byłyby zdolne do kontrolowania obszarów zagrożonych katastrofami naturalnymi w celu zapobiegania katastrofom powodującym śmierć wielu ludzi, których ekipy interweniowałyby w takich przypadkach jak ostatnia katastrofa tsunami i posiadałyby wspólne oznakowania w celu lepszego uwidocznienia solidarności europejskiej;

i) wzmocnienie partnerstwa społecznego w drodze koordynacji organizacji pozarządowych, społeczeństwa obywatelskiego i władz lokalnych;

j) zapewnienie, że ostrzeżenia, powiadomienia i noty informacyjne wydawane, aby pomóc zainteresowanym podmiotom z sektora publicznego i prywatnego w ochronie kluczowych systemów infrastrukturalnych, jak również wszelkie ostrzeżenia i powiadomienia skierowane do ogółu społeczeństwa w kontekście obrony cywilnej w stanach zagrożenia, są bezwarunkowo konieczne i adekwatne do okoliczności oraz nie zakłócają w nieuzasadniony sposób codziennego życia obywateli i funkcjonowania przedsiębiorstw, ani nie wywołują wśród ludności niepotrzebnego poczucia zagrożenia czy niepewności;

k) zapewnienie poszanowania prawa do prywatności, tak aby konsumenci i operatorzy mieli pewność, że informacje będą przetwarzane w sposób poufny, właściwy i wiarygodny, a informacje zastrzeżone przez przedsiębiorców będą prawidłowo zarządzane i chronione przed wykorzystaniem przez nieupoważnione osoby lub przed ujawnieniem;

l) zapewnienie jednoczesnego i jak najszybszego utworzenia europejskich przepisów dotyczących ochrony i przechowywania danych, wymagających ścisłego przestrzegania we wszystkich obszarach, oraz zagwarantowanie ochrony praw podstawowych;

m) zapewnienia, że ćwiczenia szkoleniowe mające na celu wzmocnienie obrony cywilnej Unii i zdolności ochrony infrastruktury o kluczowym znaczeniu prowadzone będą na podstawie realistycznych i aktualnych scenariuszy z wykorzystaniem doświadczenia i fachowej wiedzy odpowiednich specjalistów z zakresu obrony cywilnej i ochrony infrastruktury strategicznej pochodzących z Państw Członkowskich (np. ekspertów i scenariuszy z dziedziny obrony cywilnej i ochrony infrastruktury strategicznej wykorzystanych w czasie Igrzysk Olimpijskich w Atenach w 2004 r.);

2. zobowiązuje swojego Przewodniczącego do przekazania niniejszego zalecenia Radzie Europejskiej, Radzie oraz przedstawienia go do wglądu Komisji, rządom i parlamentom Państw Członkowskich, Radzie Europy oraz ONZ i jej wyspecjalizowanym agencjom.

([1]) Patrz: projekt reformy strategii obrony cywilnej i zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych omawiany na szczeblu ONZ.