KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 17.11.2005
COM(2005) 576 końcowy

ZIELONA KSIĘGA

W SPRAWIE EUROPEJSKIEGO PROGRAMU OCHRONY INFRASTRUKTURY KRYTYCZNEJ

(przedstawiony przez Komisję)

ZIELONA KSIĘGA

W SPRAWIE EUROPEJSKIEGO PROGRAMU OCHRONY INFRASTRUKTURY KRYTYCZNEJ

1. INFORMACJE OGÓLNE

Infrastruktura krytyczna (IK) może zostać uszkodzona, zniszczona lub jej działanie może ulec zakłóceniu na skutek umyślnych aktów terroryzmu, klęsk żywiołowych, zaniedbań, wypadków lub piractwa komputerowego, działalności przestępczej i działania w złej wierze. Aby chronić na terenie UE życie i mienie osób zagrożonych terroryzmem, klęskami żywiołowymi i wypadkami, należy zapewnić, by wszelkie zakłócenia lub manipulacje dotyczące IK były w miarę możliwości krótkotrwałe, rzadkie, łatwe do opanowania, odizolowane geograficznie i w jak najmniejszym stopniu szkodliwe dla dobrobytu Państw Członkowskich, ich obywateli i Unii Europejskiej. Niedawne ataki terrorystyczne w Madrycie i Londynie wykazały jasno ryzyko wystąpienia aktów terroryzmu wymierzonych przeciwko infrastrukturze europejskiej. Reakcja UE musi być szybka, skoordynowana i skuteczna.

Rada Europejska obradująca w czerwcu 2004 r zwróciła się do Komisji o opracowanie ogólnej strategii ochrony infrastruktury krytycznej. W odpowiedzi Komisja przyjęła w dniu 20 października 2004 r. komunikat pt. „Ochrona infrastruktury krytycznej w walce z terroryzmem", zawierający jasne propozycje dotyczące sposobu usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, gotowości i reakcji na takie ataki.

W konkluzjach na temat „zapobiegania atakom terrorystycznym, gotowości i reakcji" oraz w „Programie Solidarności UE na temat skutków zagrożeń i ataków terrorystycznych", przyjętym przez Radę w grudniu 2004 r., Rada poparła zamiar Komisji dotyczący przedstawienia Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK) i wyraziła zgodę na utworzenie przez Komisję sieciowego systemu ostrzegania o zagrożeniach dotyczących infrastruktury krytycznej (ang. *Critical Infrastructure Warning Information Network* – CIWIN).

Komisja zorganizowała dwa seminaria i zaprosiła Państwa Członkowskie do zgłaszania pomysłów i uwag. Pierwsze seminarium w sprawie ochrony infrastruktury krytycznej w UE odbyło się w dniach 6-7 czerwca 2005 r. z udziałem Państw Członkowskich. W następstwie tego seminarium Państwa Członkowskie przekazały Komisji odpowiednią dokumentację ogólną dotyczącą swojego podejścia do ochrony infrastruktury krytycznej (OIK) oraz uwagi na temat koncepcji omawianych podczas seminarium. Dokumentacja, którą Komisja otrzymała w czerwcu i lipcu, posłużyła jako podstawa do dalszych prac nad OIK. W dniach 12-13 września zorganizowano drugie seminarium poświęcone OIK w celu posunięcia naprzód dyskusji dotyczącej ochrony infrastruktury krytycznej. W seminarium tym wzięły udział Państwa Członkowskie i stowarzyszenia branżowe. Jego skutkiem była decyzja Komisji o opracowaniu niniejszej zielonej księgi przedstawiającej możliwości działania EPOIK.

2. CEL ZIELONEJ KSIĘGI

Głównym celem zielonej księgi jest zdobycie informacji dotyczących możliwych opcji polityki EPOIK poprzez zaangażowanie dużej liczby zainteresowanych stron. Skuteczna ochrona infrastruktury krytycznej wymaga komunikacji, koordynacji i współpracy na poziomie krajowym i unijnym pomiędzy wszystkimi zainteresowanymi stronami – właścicielami i operatorami infrastruktury, organami regulacji, organizacjami zawodowymi i stowarzyszeniami branżowymi – we współpracy ze wszystkimi poziomami władz państwowych oraz ogółem społeczeństwa.

Zielona księga dostarcza informacji na temat tego, jak Komisja może odpowiedzieć na wniosek Rady o utworzenie EPOIK i CIWIN i stanowi drugą fazę procesu konsultacji dotyczącego ustanowienia Europejskiego Programu Ochrony Infrastruktury Krytycznej. Komisja oczekuje, że dzięki przedstawieniu niniejszej zielonej księgi otrzyma konkretne informacje dotyczące możliwości rozwiązań politycznych opisanych w niniejszym dokumencie. W zależności od wyniku procesu konsultacji pakiet wytycznych EPOIK mógłby zostać przedstawiony w 2006 r.

3. CEL I ZAKRES EPOIK

3.1. Ogólny cel EPOIK

Celem EPOIK byłoby zapewnienie istnienia odpowiednich i jednakowych poziomów zabezpieczeń ochronnych w zakresie infrastruktury krytycznej, ograniczenie przypadków awarii do minimum oraz dostarczenie szybkich i sprawdzonych środków naprawczych w całej Unii. Poziom ochrony może nie być jednakowy dla wszystkich rodzajów IK i może być uzależniony od wagi skutków ewentualnej awarii infrastruktury krytycznej. EPOIK byłby ciągłym procesem, wymagającym systematycznego przeglądu w celu uwzględnienia nowych zagadnień i obaw.

EPOIK powinien w największym możliwym stopniu minimalizować negatywny wpływ, jaki zwiększenie inwestycji w bezpieczeństwo mogłoby wywierać na konkurencyjność danej branży przemysłu. Przy obliczaniu proporcjonalności kosztów nie należy zapominać o potrzebie utrzymania stabilności rynkowej, kluczowej dla inwestycji długoterminowych, o wpływie bezpieczeństwa na zmiany sytuacji giełdowej i na wymiar makroekonomiczny.

Pytanie

Czy tak określony cel jest odpowiedni dla EPOIK? Jeżeli nie, co powinno być celem programu?

3.2. Przed czym EPOIK powinien chronić

Chociaż środki zarządzania skutkami są jednakowe lub podobne dla większości przypadków zakłóceń, środki ochronne mogą się różnić w zależności od charakteru zagrożenia. Do zagrożeń mogących znacznie zmniejszyć zdolność do zaspokojenia podstawowych potrzeb populacji, zapewnienia bezpieczeństwa, utrzymania porządku i świadczenia minimum niezbędnych usług publicznych lub sprawnego funkcjonowania gospodarki zaliczają się umyślne ataki i klęski żywiołowe. Istnieją następujące możliwości:

a) **ogólne podejście obejmujące wszystkie rodzaje ryzyka** – stanowiłoby ono ogólne podejście uwzględniające zarówno zagrożenia stwarzane przez ataki umyślne, jak i klęski żywiołowe. Zapewniłoby ono maksymalne wykorzystanie synergii pomiędzy środkami ochronnymi, ale nie kładłoby szczególnego nacisku na problem terroryzmu;

b) **podejście obejmujące wszystkie rodzaje ryzyka ze szczególnym uwzględnieniem terroryzmu** – byłoby to podejście elastyczne, uwzględniające inne rodzaje zagrożeń, takie jak zagrożenie atakami umyślnymi oraz klęskami żywiołowymi, ale jego priorytetem byłby problem terroryzmu. Jeżeli poziom środków ochronnych w danym sektorze przemysłu uznano by za odpowiedni, zainteresowane strony skupiłyby uwagę na zagrożeniach, na które nadal są podatne;

c) **podejście obejmujące ryzyko związane z terroryzmem** – byłoby to podejście skupione na terroryzmie, nieuwzględniające w szczególny sposób bardziej powszechnych zagrożeń.

Pytanie

Które podejście powinien obrać EPOIK? Dlaczego?

4. PROPONOWANE KLUCZOWE ZASADY

Proponuje się następujące kluczowe zasady mające stanowić podstawę EPOIK:

- **Pomocniczość** – pomocniczość byłaby centralną zasadą EPOIK stanowiącą, że ochrona infrastruktury krytycznej leży przede wszystkim w kompetencji władz krajowych. Główna odpowiedzialność za ochronę infrastruktury krytycznej spoczywałaby na Państwach Członkowskich i właścicielach/operatorach działających według wspólnych ram. Komisja z kolei skupiłaby się na aspektach związanych z ochroną infrastruktury krytycznej mającej charakter transgraniczny. Odpowiedzialność właścicieli i operatorów za podejmowanie własnych decyzji i opracowywanie planów ochrony swojego mienia nie powinna ulec zmianie.

- **Komplementarność** – wspólne ramy EPOIK stanowiłyby uzupełnienie istniejących środków. Tam, gdzie już działają mechanizmy wspólnotowe, powinno się nadal z nich korzystać, gdyż pomagają one w ogólnej realizacji EPOIK.

- **Poufność** – wymiana informacji dotyczących ochrony infrastruktury krytycznej odbywałaby się w atmosferze zaufania i poufności. Jest to konieczne, jeżeli weźmie się pod uwagę fakt, że szczególne informacje dotyczące infrastruktury krytycznej mogą zostać wykorzystane w celu spowodowania awarii lub wywołania niedopuszczalnych skutków w urządzeniach infrastruktury krytycznej. Informacje byłyby zastrzeżone na poziomie UE i Państw Członkowskich, a dostęp do nich przyznawano by jedynie w koniecznych przypadkach.

- **Współpraca zainteresowanych stron** – wszystkie zainteresowane strony, w tym Państwa Członkowskie, Komisja, stowarzyszenia branżowe, organy normalizacyjne, właściciele, operatorzy i użytkownicy (przez „użytkownika” rozumie się organizacje wykorzystujące infrastrukturę do celów zawodowych i do celów świadczenia usług) mają rolę do odegrania w ochronie IK. Wszystkie zainteresowane strony powinny współpracować i przyczyniać się do rozwoju i realizacji EPOIK zgodnie ze swoją szczególną rolą i odpowiedzialnością.

Władze Państw Członkowskich przewodniczyłyby pracom nad spójnym krajowym podejściem do ochrony infrastruktury krytycznej i procesowi jego wdrażania oraz koordynowały te działania na obszarze swojej właściwości. Właściciele, operatorzy i użytkownicy aktywnie wspieraliby te działania na poziomie krajowym i UE. W dziedzinach, w których normy sektorowe nie istnieją lub nie ustanowiono jeszcze norm międzynarodowych, organizacje normalizacyjne mogłyby w stosownych przypadkach przyjąć wspólne normy.

- **Proporcjonalność** – strategie i środki ochronne byłyby proporcjonalne do poziomu ryzyka, ponieważ nie wszystkie rodzaje infrastruktury mogą być chronione przed wszystkimi zagrożeniami (na przykład sieci transmisji elektrycznej są zbyt duże, aby można je było ogrodzić lub zabezpieczyć). Dzięki zastosowaniu odpowiednich technik zarządzania ryzykiem szczególna uwaga poświęcono by obszarom największego ryzyka, przy uwzględnieniu zagrożenia, względnej krytyczności, stosunku kosztów do korzyści, poziomu zabezpieczeń ochronnych i skuteczności dostępnych strategii łagodzenia skutków.

Pytanie

Czy wymienione kluczowe zasady są do przyjęcia? Czy niektóre z nich są zbędne? Czy istnieją inne zasady, które należałoby rozważyć?

Czy zgadzają się Państwo, że środki ochronne powinny być proporcjonalne do poziomu ryzyka, ponieważ nie wszystkie rodzaje infrastruktury mogą być chronione przed wszystkimi zagrożeniami?

5. WSPÓLNE RAMY EPOIK

Uszkodzenie lub utrata części infrastruktury w jednym Państwie Członkowskim może wywrzeć negatywny wpływ na inne państwa oraz na gospodarkę europejską. 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 rodzajów infrastruktury stanowi część większej sieci. W takiej sytuacji środki ochronne są jedynie tak mocne, jak mocne jest ich najsłabsze ogniwo. Oznacza to, że konieczne może okazać się utworzenie wspólnego poziomu ochrony.

Skuteczna ochrona wymaga komunikacji, koordynacji i współpracy pomiędzy wszystkimi zainteresowanymi stronami na poziomie krajowym, unijnym (w stosownych przypadkach) oraz międzynarodowym. Można by wdrożyć wspólne ramy ochrony infrastruktury krytycznej w Europie na poziomie UE w celu zapewnienia odpowiedniego i jednakowego poziomu ochrony infrastruktury krytycznej we wszystkich Państwach Członkowskich oraz przestrzegania zasad konkurencji na rynku wewnętrznym. W celu wsparcia działań Państw Członkowskich Komisja ułatwiłaby ustalenie, wymianę i rozpowszechnianie najlepszych praktyk w dziedzinach związanych z ochroną infrastruktury krytycznej poprzez opracowanie wspólnych ram ochrony infrastruktury krytycznej. Należy rozważyć zakres tych ogólnych ram.

Wspólne ramy EPOIK obejmowałyby środki horyzontalne definiujące kompetencje i odpowiedzialność wszystkich zainteresowanych stron w dziedzinie ochrony infrastruktury krytycznej (OIK) oraz stanowiące podstawę dla opracowania odrębnego podejścia dla każdego sektora. Wspólne ramy mają uzupełnić istniejące środki sektorowe na poziomie wspólnotowym i w Państwach Członkowskich w celu zapewnienia najwyższego możliwego poziomu bezpieczeństwa infrastruktury krytycznej w Unii Europejskiej. Należy przyznać priorytet pracom nad osiągnięciem porozumienia w kwestii wspólnego wykazu definicji i sektorów IK.

Ponieważ sektory zawierające infrastrukturę krytyczną są bardzo zróżnicowane, trudno byłoby dokładnie ustalić, jakimi kryteriami należy się kierować w celu wyznaczenia i ochrony wszystkich z nich w ramach horyzontalnych; należy zatem tego dokonać osobno dla każdego sektora. Jednakże istnieje potrzeba wspólnego zrozumienia pewnych kwestii przekrojowych.

W związku z tym proponuje się wzmocnienie infrastruktury krytycznej w UE poprzez ustalenie wspólnych ram EPOIK (wspólnych celów, metodologii służącej np. do celów porównawczych, współzależności), wymianę najlepszych praktyk i ustanowienie mechanizmów kontroli zgodności. Do elementów składających się na wspólne ramy zaliczałyby się:

- wspólne zasady OIK;
- wspólnie ustalone kody/normy
- wspólne definicje, na podstawie których można ustalić definicje dla poszczególnych sektorów (orientacyjny wykaz definicji zawarty jest w załączniku 1);
- wspólny wykaz sektorów IK (orientacyjny wykaz sektorów zawarty jest w załączniku 2);
- obszary priorytetowe OIK;
- opis zakresu odpowiedzialności zainteresowanych stron;
- ustalone wskaźniki;
- metodologia służąca porównaniu i przyznaniu priorytetowego znaczenia infrastrukturze w różnych sektorach;

Takie wspólne ramy zmniejszyłyby również możliwe zakłócenia na rynku wewnętrznym.

Wspólne ramy EPOIK mogłyby być dobrowolne bądź obowiązkowe – lub „mieszane” w zależności od przypadku. Oba rodzaje ram mogłyby uzupełniać istniejące środki sektorowe i horyzontalne na poziomie Wspólnoty i Państw Członkowskich, jednak wyłącznie ramy prawne stanowiłyby silną i egzekwowalną podstawę prawną spójnego i jednolitego procesu wdrażania działań służących ochronie EIK oraz określiłyby jasno zakres odpowiedzialności Państw Członkowskich i Komisji. Ze względu na swoją elastyczność niewiążące i dobrowolne środki nie określałyby jasno, co jest czyim zadaniem.

W zależności od wyniku uważnej analizy i w dążeniu do ustalenia proporcjonalności proponowanych środków Komisja może wykorzystać w swoim wniosku dotyczącym EPOIK liczne instrumenty, w tym prawodawstwo. W stosownych przypadkach wnioskom dotyczącym zastosowania szczególnych środków będą towarzyszyć oceny wpływu.

Pytania

Czy wspólne ramy skutecznie wzmocniłyby OIK?

Jeżeli potrzebne są ramy prawne, jakie elementy powinny one zawierać?

Czy zgadzają się Państwo, że kryteria określania różnych rodzajów EIK oraz środki ochronne uważane za konieczne powinny zostać ustalone dla poszczególnych sektorów?

Czy wspólne ramy okazałyby się pomocne w objaśnieniu zakresu odpowiedzialności zainteresowanych stron? W jakim stopniu takie wspólne ramy powinny być obowiązkowe, a w jakim – dobrowolne?

Jaki powinien być zakres wspólnych ram? Czy zgadzają się Państwo z wykazem orientacyjnych terminów i definicji w załączniku I, na podstawie którego w stosownych przypadkach mogą zostać opracowane definicje dla poszczególnych sektorów? Czy zgadzają się Państwo z wykazem orientacyjnych sektorów IK w załączniku II?

6. INFRASTRUKTURA KRYTYCZNA UE (EIK)

6.1. Definicja infrastruktury krytycznej UE

Określenie tego, co stanowi infrastrukturę krytyczną UE, zależeć będzie od jej charakteru transgranicznego, czyli ustalenia, czy ewentualny incydent mógłby mieć poważne skutki poza terytorium Państwa Członkowskiego, na którym urządzenia się znajdują. Innym elementem, który należy tu wziąć pod uwagę, jest fakt, że dwustronne programy współpracy dotyczące OIK, zawierane pomiędzy Państwami Członkowskimi, stanowią sprawdzony i skuteczny środek rozwiązywania problemów w dziedzinie IK znajdujących się na obszarze dwóch Państw Członkowskich. Tego typu współpraca stanowiłaby uzupełnienie EPOIK.

Do EIK mogłyby zaliczać się zasoby fizyczne, usługi, sprzęt informatyczny, sieci i aktywa infrastruktury, których zakłócenie lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo, dobrobyt gospodarczy lub społeczny:

a) dwóch lub większej liczby Państw Członkowskich – **obejmowałoby to niektóre rodzaje IK o charakterze dwustronnym (w stosownych przypadkach)**;

b) trzech lub większej liczby Państw Członkowskich – **wykluczałoby to wszelkie IK o charakterze dwustronnym**;

Przy rozważaniu korzyści płynących z obu tych możliwości należy uwzględnić następujące kwestie:

– fakt, że dana infrastruktura zostanie uznana za EIK, nie oznacza, że będzie ona wymagać zastosowania dodatkowych środków ochronnych. Istniejące środki ochronne, do których mogą zaliczać się porozumienia dwustronne pomiędzy Państwami Członkowskimi, mogą

być całkowicie wystarczające i w związku z tym pozostać niezmienione po oznaczeniu infrastruktury jako EIK;

– wybór możliwości a) może pociągnąć za sobą dużą liczbę oznaczeń;

– wybór możliwości b) może oznaczać, że infrastruktura mająca znaczenie jedynie dla dwóch Państw Członkowskich nie otrzyma wsparcia ze strony Wspólnoty, nawet jeżeli poziom ochrony uważany jest za niewystarczający przez jedno z tych dwóch Państw Członkowskich, a drugie odmówiło podjęcia działań. Wybór możliwości b) mógłby również doprowadzić do powstania wielu dwustronnych porozumień lub nieporozumień pomiędzy Państwami Członkowskimi. Przemysł, który często ma charakter ogólnoeuropejski, byłby zmuszony dostosowywać się do różnych porozumień, co mogłoby pociągnąć za sobą dodatkowe koszty.

Ponadto uznaje się, że należy również uwzględnić IK pochodzącą spoza UE lub istniejącą poza nią, ale współzależną lub mogącą bezpośrednio oddziaływać na Państwa Członkowskie UE.

Pytanie

Czy za EIK powinno się uznać infrastrukturę mogącą wywierać poważny wpływ o charakterze transgranicznym na dwa lub większą liczbę czy też na trzy lub większą liczbę Państw Członkowskich? Dlaczego?

6.2. Współzależność

Proponuje się, aby stopniowe oznaczanie wszystkich EIK uwzględniało w szczególności współzależność. Analizy współzależności wniosłyby wkład do oceny potencjalnego wpływu zagrożeń dotyczących poszczególnych rodzajów IK i w szczególności pomogłyby ustalić, które Państwo Członkowskie ucierpiałoby w przypadku poważnego incydentu związanego z IK.

Pod uwagę wzięto by współzależność w przedsiębiorstwach, sektorach przemysłu, obszarach właściwości geograficznej i organach władzy Państw Członkowskich, zwracając szczególną uwagę na te mające dostęp do technologii informacyjnych i komunikacyjnych – oraz pomiędzy wszystkimi tymi elementami. Komisja, Państwa Członkowskie i właściciele/operatorzy infrastruktury krytycznej podjęliby wspólne działania w celu określenia tych rodzajów współzależności i zastosowania odpowiednich strategii służących zmniejszeniu – tam, gdzie to możliwe – ryzyka.

Pytanie

W jaki sposób można uwzględniać współzależność?

Czy znają Państwo odpowiednią metodologię służącą do analizy współzależności?

Na jakim poziomie powinno odbywać się ustalenie współzależności – na poziomie UE i/lub Państw Członkowskich?

6.3. Etapy wdrażania programu EIK

Komisja proponuje następujące etapy wdrażania programu EIK:

(1) Komisja wraz z Państwami Członkowskimi opracowuje szczególne kryteria, które zostaną wykorzystane do oznaczenia EIK w poszczególnych sektorach;

(2) Stopniowe oznaczanie i kontrola EIK w poszczególnych sektorach przez Państwa Członkowskie i Komisję. Decyzja o uznaniu konkretnych przypadków IK za EIK podejmowana jest na poziomie europejskim[1] z uwagi na transgraniczny charakter danej infrastruktury;

(3) Państwa Członkowskie i Komisja analizują istniejące luki w systemie bezpieczeństwa związane z EIK w poszczególnych sektorach;

(4) Państwa Członkowskie i Komisja uwzględniają współzależność i uzgadniają sektory priorytetowe/infrastrukturę priorytetową, w związku z którymi zostaną podjęte działania;

(5) W stosownych przypadkach dla każdego sektora Komisja i najważniejsze zainteresowane strony z Państw Członkowskich uzgadniają wnioski dotyczące minimalnych środków ochronnych, do których mogłyby zaliczać się normy;

(6) Po przyjęciu wniosków przez Radę środki te zostają wdrożone;

(7) Państwa Członkowskie i Komisja prowadzą systematyczne kontrole. Przeglądów (środków i oznaczeń IK) dokonuje się we właściwym czasie i w stosownych przypadkach.

Pytania

Czy wykaz etapów wdrażania programu EIK jest do przyjęcia?

W jaki sposób Państwa zdaniem Komisja i Państwa Członkowskie powinny wspólnie dokonywać oznaczenia EIK – na podstawie wiedzy specjalistycznej Państw Członkowskich i spojrzenia Komisji z perspektywy interesu europejskiego? Czy powinna to być decyzja prawnie wiążąca?

Czy istnieje potrzeba ustanowienia mechanizmu arbitrażowego na wypadek, gdyby dane Państwo Członkowskie nie zgadzało się na oznaczenie IK znajdującej się na obszarze jego właściwości jako EIK?

Czy istnieje potrzeba kontroli oznaczeń? Kto powinien ponosić odpowiedzialność?

Czy Państwo Członkowskie powinno mieć prawo do oznaczenia infrastruktury znajdującej się w innym Państwie Członkowskim lub w państwach trzecich jako krytycznej dla siebie? Co należy zrobić, jeżeli Państwo Członkowskie, państwo trzecie lub branża przemysłu uważa infrastrukturę w danym Państwie Członkowskim za krytyczną dla siebie?

[1] Z wyjątkiem infrastruktury związanej z obroną.

Co należy zrobić, jeżeli w takim wypadku to Państwo Członkowskie nie oznaczy jej? Czy istnieje potrzeba ustanowienia mechanizmu odwoławczego? Jeżeli tak, to jakiego rodzaju?

Czy operator powinien mieć prawo odwołania się, jeżeli nie zgadza się on na oznaczenie lub brak oznaczenia? Jeżeli tak, to do kogo?

Jaką metodologię należałoby opracować w celu ustalenia sektorów priorytetowych/infrastruktury priorytetowej, w związku z którymi zostaną podjęte działania? Czy istnieją już odpowiednie rodzaje metodologii, które można dostosować do poziomu europejskiego?

W jaki sposób Komisja może uczestniczyć w analizie luk w systemie bezpieczeństwa związanych z EIK?

7. KRAJOWA INFRASTRUKTURA KRYTYCZNA (KIK)

7.1. Rola KIK w EPOIK

Wiele przedsiębiorstw europejskich prowadzi działalność o charakterze transgranicznym i jako takie podlega różnym zobowiązaniom nałożonym na KIK. Proponuje się zatem w interesie Państw Członkowskich i UE jako całości, aby każde Państwo Członkowskie chroniło swoją KIK zgodnie ze wspólnymi ramami, tak aby właściciele i operatorzy w całej Europie nie musieli podlegać różnym ramom powodującym różnorodność metodologii i dodatkowe koszty. W związku z tym Komisja uważa, że EPOIK, skupiający się przede wszystkim na infrastrukturze krytycznej UE, nie może całkowicie wykluczać krajowej infrastruktury krytycznej. Istnieją jednak trzy możliwości:

a) KIK jest w całości objęta EPOIK;

b) KIK jest poza zakresem EPOIK;

c) Państwa Członkowskie mogą, ale nie muszą, częściowo wykorzystywać EPOIK w odniesieniu do KIK według własnego uznania.

Pytanie

Wydaje się, że skuteczna ochrona infrastruktury krytycznej w Unii Europejskiej wymaga oznaczenia zarówno EIK, jak i KIK. Czy zgadzają się Państwo, że chociaż EPOIK winien skupić się na EIK, KIK nie powinna zostać całkowicie wykluczona?

Która z wymienionych możliwości Państwa zdaniem jest najodpowiedniejsza dla EPOIK?

7.2. Krajowe programy OIK

W oparciu o wspólne ramy EPOIK Państwa Członkowskie mogłyby opracować krajowe programy OIK dla swojej KIK. Państwa Członkowskie byłyby w stanie zastosować bardziej rygorystyczne środki niż te przewidziane w ramach EPOIK.

Pytanie

Czy każde Państwo Członkowskie powinno przyjąć krajowy program OIK oparty na EPOIK?

7.3. Jeden organ nadzorczy

W związku z potrzebą skuteczności i spójności Państwa Członkowskie powinny wyznaczyć jeden organ nadzorczy, którego zadaniem byłaby ogólna realizacja EPOIK. Można rozważyć dwie możliwości:

a) Jeden organ nadzorczy w dziedzinie OIK;

b) Krajowy punkt kontaktowy, który nie posiada żadnej władzy i pozostawia organizację Państwom Członkowskim.

Taki organ mógłby koordynować, kontrolować i nadzorować realizację EPOIK na obszarze swojej właściwości i mógłby służyć jako główny instytucjonalny punkt do kontaktów z Komisją, innymi Państwami Członkowskimi, właścicielami i operatorami IK w kwestiach OIK. Organ ten mógłby stanowić podstawę reprezentacji krajowej w grupach specjalistycznych zajmujących się kwestiami OIK i mógłby być połączony z sieciowym systemem ostrzegania o zagrożeniach dotyczących infrastruktury krytycznej (CIWIN). Krajowy organ koordynacji OIK (KOK) mógłby koordynować krajowe kwestie OIK niezależnie od innych organów lub podmiotów w danym Państwie Członkowskim, które mogą już być zaangażowane w sprawy OIK.

Stopniowe oznaczanie KIK mogłoby dokonywać się poprzez zobowiązanie właścicieli i operatorów infrastruktury do zawiadamiania KOK o wszelkiej działalności zawodowej związanej z OIK.

KOK mógłby być odpowiedzialny za podejmowanie prawnie wiążącej decyzji w sprawie oznaczenia infrastruktury znajdującej się na obszarze jego właściwości jako KIK. Informacją tą dysponowałoby jedynie dane Państwo Członkowskie.

Do szczególnych kompetencji KOK mogłyby się zaliczać:

a) koordynacja, kontrola i nadzór ogólnej realizacji EPOIK w danym Państwie Członkowskim;

b) pełnienie funkcji głównego instytucjonalnego punktu ds. OIK w kontaktach z:

   i) Komisją,

   ii) innymi Państwami Członkowskimi,

   iii) właścicielami i operatorami IK;

c) udział w oznaczaniu infrastruktury krytycznej UE (EIK);

d) podejmowanie prawnie wiążących decyzji o oznaczeniu infrastruktury znajdującej się na obszarze jego właściwości jako krajowej infrastruktury krytycznej;

e) pełnienie funkcji organu odwoławczego dla właścicieli/operatorów, którzy nie zgadzają się na oznaczenie ich infrastruktury jako „infrastruktury krytycznej”;

f) udział w opracowywaniu programu ochrony krajowej infrastruktury krytycznej i programów OIK dla poszczególnych sektorów;

g) określanie współzależności między poszczególnymi sektorami IK;

h) wkład w opracowanie podejść dotyczących OIK dla poszczególnych sektorów poprzez przynależność do grup specjalistycznych. Przedstawiciele właścicieli i operatorów mogliby zostać zaproszeni do udziału w dyskusji. Można by organizować regularne spotkania;

i) Nadzorowanie procesu opracowywania planów działań w sytuacjach zagrożenia związanych z IK.

Pytania

Czy zgadzają się Państwo, aby wyłącznie Państwa Członkowskie były odpowiedzialne za oznaczanie KIK i zarządzanie nią zgodnie ze wspólnymi ramami EPOIK?

Czy należy wyznaczyć organ koordynacji OIK w każdym Państwie Członkowskim, ponoszący całkowitą odpowiedzialność za koordynację środków związanych z OIK, przy jednoczesnym poszanowaniu istniejącego zakresu odpowiedzialności poszczególnych sektorów (władze lotnictwa cywilnego, dyrektywa Seveso itp.)?

Czy zaproponowane kompetencje takiego organu koordynacyjnego są odpowiednie? Czy istnieją inne, które należałoby mu nadać?

7.4. Etapy wdrażania programu KIK

Komisja proponuje następujące etapy wdrażania programu KIK:

(1) korzystając z EPOIK, Państwa Członkowskie opracowują szczególne kryteria, które zostaną użyte do oznaczenia KIK;

(2) stopniowe oznaczanie i kontrola KIK w poszczególnych sektorach przez Państwa Członkowskie;

(3) Państwa Członkowskie analizują istniejące luki w systemie bezpieczeństwie związane z KIK w poszczególnych sektorach;

(4) Państwa Członkowskie ustalają sektory priorytetowe, w których zostaną podjęte działania, przy uwzględnieniu współzależności i, w stosownych przypadkach, uzgodnionych priorytetów na poziomie UE;

(5) w stosownych przypadkach dla każdego sektora Państwa Członkowskie ustalają minimalne środki ochronne;

(6) Państwa Członkowskie ponoszą odpowiedzialność na swoim obszarze właściwości za przeprowadzenie przez właścicieli/operatorów niezbędnych działań związanych z wdrażaniem;

(7) Państwa Członkowskie prowadzą systematyczne kontrole. Dokonuje się przeglądów (środków i oznaczeń IK) we właściwym czasie i w stosownych przypadkach.

Pytanie

Czy wykaz etapów wdrażania programu KIK jest odpowiedni? Czy jakieś etapy są zbędne? Czy powinno się dodać jakieś etapy?

8. ROLA WŁAŚCICIELI, OPERATORÓW I UŻYTKOWNIKÓW IK

8.1. Obowiązki właścicieli, operatorów i użytkowników IK

Oznaczenie jako IK oznacza dla właścicieli i operatorów pewne dodatkowe obowiązki. Można wyróżnić cztery rodzaje obowiązków właścicieli i operatorów infrastruktury oznaczonej jako KIK lub EIK:

(1) zgłaszanie odpowiedniemu organowi OIK Państwa Członkowskiego faktu, że dana infrastruktura może mieć charakter krytyczny;

(2) **mianowanie wyższego(-ych) rangą przedstawiciela(-i) na stanowisko oficera łącznikowego ds. bezpieczeństwa (OŁB) do kontaktów pomiędzy właścicielem/operatorem a odpowiednim organem OIK Państwa Członkowskiego**. OŁB brałby udział w opracowywaniu planów bezpieczeństwa i planów działań w sytuacjach zagrożenia. OŁB byłby głównym oficerem łącznikowym do kontaktów z odpowiednim organem sektora OIK w Państwie Członkowskim i w stosownych przypadkach do kontaktów z organami ścigania;

(3) **opracowanie, realizacja i aktualizacja Planu Bezpieczeństwa Operatorów (PBO).** Proponowany wzór PBO jest zamieszczony w załączniku 3.

(4) **udział w opracowaniu planu działań w sytuacjach zagrożenia** związanych z IK wspólnie z odpowiednimi organami ochrony cywilnej i z organami ścigania Państw Członkowskich, jeżeli wyrażą one taką wolę.

PBO mógłby zostać przedłożony do aprobaty odpowiedniemu organowi OIK Państwa Członkowskiego pod ogólnym nadzorem KOK, niezależnie od tego, czy chodzi o KIK, czy EIK. Zapewniłoby to spójność działań na rzecz bezpieczeństwa podejmowanych przez poszczególnych właścicieli i operatorów i ogólnie przez odpowiednie sektory. Z kolei właściciele i operatorzy mogliby otrzymywać istotne informacje i wsparcie w odniesieniu do znaczących zagrożeń oraz przy tworzeniu najlepszych praktyk, a w stosownych przypadkach pomoc w ocenie współzależności i podatności na zagrożenia ze strony KOK i Komisji.

Każde Państwo Członkowskie mogłoby ustalić termin sporządzenia PBO przez właścicieli i operatorów KIK i EIK (w przypadku EIK zaangażowana byłaby również Komisja) i nakładać kary administracyjne za nieprzestrzeganie tego terminu.

Proponuje się, aby Plan Bezpieczeństwa Operatorów (PBO) określał aktywa infrastruktury krytycznej właściciela/operatora i proponował odpowiednie zabezpieczenia w celu ich ochrony. PBO przedstawiłby metody i procedury, które należy stosować w celu zapewnienia zgodności z EPOIK, krajowymi programami OIK i odpowiednimi programami OIK dla poszczególnych sektorów. PBO mógłby być narzędziem podejścia oddolnego do kwestii nadzoru OIK, przyznającego więcej swobody (i również więcej odpowiedzialności) sektorowi prywatnemu.

W szczególnych sytuacjach, gdy chodzi o niektóre rodzaje infrastruktury, takie jak sieci elektryczne i sieci informacyjne, oczekiwanie, że właściciele i operatorzy zapewnią jednakowy poziom zabezpieczeń wszystkich swoich aktywów byłoby mało realistyczne (z praktycznego i finansowego punktu widzenia). W takich przypadkach proponuje się, aby właściciele i operatorzy wraz z odpowiednimi organami władzy określali punkty krytyczne (węzły) sieci fizycznej lub informacyjnej, na których winny skupić się działania związane z ochroną bezpieczeństwa.

PBO mógłby obejmować środki bezpieczeństwa podzielone na dwie następujące kategorie:

- **stałe środki bezpieczeństwa**, określające niezbędne inwestycje i środki w dziedzinie bezpieczeństwa, które nie mogą zostać zainstalowane przez właściciela/operatora w krótkim czasie. Właściciel/operator utrzymywałby stan gotowości na wypadek potencjalnych zagrożeń, co nie zakłóciłoby jego zwykłej działalności gospodarczej, administracyjnej i społecznej.

- **progresywne środki bezpieczeństwa**, które można by aktywować zależnie od różnych poziomów zagrożenia. PBO określałby różne systemy bezpieczeństwa dostosowane do możliwych poziomów zagrożeń istniejących w Państwach Członkowskich, w których znajduje się strategiczny element infrastruktury.

Proponuje się, aby w razie niedostosowania się właściciela lub operatora do obowiązku opracowania PBO, udziału w opracowywaniu planów działań w sytuacjach zagrożenia i wyznaczeniu OŁB istniała możliwość nałożenia na niego kary finansowej.

Pytania

Czy potencjalne obowiązki właścicieli/operatorów infrastruktury krytycznej są do przyjęcia z perspektywy dążenia do zwiększenia bezpieczeństwa infrastruktury krytycznej? Jaki byłby ich prawdopodobny koszt?

Czy właściciele i operatorzy powinni mieć obowiązek zgłaszania faktu, że ich infrastruktura może mieć charakter krytyczny? Czy uważają Państwo koncepcję PBO za przydatną? Dlaczego?

Czy proponowane obowiązki są proporcjonalne do kosztów?

Jakie prawa mogłyby przyznać władze Państw Członkowskich oraz Komisja właścicielom i operatorom IK?

8.2. Dialog z właścicielami, operatorami i użytkownikami IK

EPOIK mógłby zaangażować właścicieli i operatorów w przedsięwzięcia partnerskie. Powodzenie jakiegokolwiek programu ochrony zależy od współpracy i poziomu zaangażowania właścicieli i operatorów, jaki można osiągnąć. Na terenie Państwa Członkowskiego właściciele i operatorzy IK mogliby być mocno zaangażowani w rozwój OIK poprzez regularne kontakty z KOK.

Na poziomie UE można by utworzyć fora w celu ułatwienia wymiany poglądów w kwestiach OIK zarówno ogólnych, jak i dotyczących poszczególnych sektorów. Wspólne podejście do kwestii zaangażowania sektora prywatnego w sprawy związane z OIK, mające na celu zebranie wszystkich zainteresowanych stron w sferze publicznej i prywatnej, dałoby Państwom Członkowskim, Komisji i przemysłowi ważne narzędzie komunikacji na temat wszelkich nowych zagadnień związanych z OIK. Właściciele, operatorzy i użytkownicy IK mogliby brać udział w opracowaniu wspólnych wytycznych, norm dotyczących najlepszych praktyk i w stosownych przypadkach w wymianie istotnych informacji. Tego typu dialog pomógłby w dokonywaniu przeglądów EPOIK w przyszłości.

W stosownych przypadkach Komisja mogłaby zachęcać do tworzenia unijnych stowarzyszeń branżowych/stowarzyszeń przedsiębiorców w związku z OIK. Dwoma ostatecznymi celami byłoby zapewnienie utrzymania konkurencyjności przez przemysł europejski i zwiększenie bezpieczeństwa obywateli UE.

Pytanie

Jak powinien być zorganizowany dialog z właścicielami, operatorami i użytkownikami IK?

Kto powinien reprezentować właścicieli, operatorów i użytkowników w dialogu publiczno-prywatnym?

9. ŚRODKI WSPIERAJĄCE EPOIK

9.1. Sieciowy system ostrzegania o zagrożeniach dotyczących infrastruktury krytycznej (CIWIN)

Komisja opracowała wiele systemów wczesnego ostrzegania pozwalających na konkretną, skoordynowaną i skuteczną odpowiedź w razie sytuacji wyjątkowych, w tym sytuacji związanych z terroryzmem. W dniu 20 października 2004 r. Komisja ogłosiła utworzenie centralnej sieci w Komisji zapewniającej szybki przepływ informacji pomiędzy wszystkimi systemami wczesnego ostrzegania Komisji i danych służb Komisji (ARGUS).

Komisja proponuje utworzenie CIWIN, który mógłby wspomagać tworzenie odpowiednich środków ochronnych poprzez ułatwienie wymiany najlepszych praktyk w bezpieczny sposób i byłby narzędziem przekazu informacji o natychmiastowych zagrożeniach oraz sygnałów ostrzegawczych. System ten zapewniałby odpowiednim osobom dostęp do właściwych informacji we właściwym czasie.

Możliwe są trzy następujące opcje dotyczące utworzenia CIWIN:

(1) CIWIN byłby forum o działaniu ograniczonym do wymiany koncepcji dotyczących OIK i najlepszych praktyk w celu udzielenia wsparcia właścicielom i operatorom IK. Takie forum mogłoby przyjąć formę sieci specjalistów i dysponować portalem elektronicznym do wymiany istotnych informacji w bezpiecznym środowisku. Komisja odgrywałaby ważną rolę w gromadzeniu i rozpowszechnianiu takich informacji. Opcja ta nie zapewniłaby koniecznego wczesnego ostrzegania o zbliżających się zagrożeniach. Jednakże CIWIN mógłby w przyszłości poszerzyć swój zakres działalności.

(2) **CIWIN byłby systemem wczesnego ostrzegania (SWO), łączącym Państwa Członkowskie z Komisją.** Realizacja tej opcji oznaczałaby, że bezpieczeństwo infrastruktury krytycznej zostałoby zwiększone poprzez dostarczanie sygnałów ostrzegawczych i ostrzeżeń ograniczonych do natychmiastowych zagrożeń. Celem byłoby ułatwienie właścicielom i operatorom IK szybkiej wymiany informacji o potencjalnych zagrożeniach. SWO nie obejmowałby wymiany danych wywiadowczych obejmujących dłuższy okres. Byłby on używany do szybkiej wymiany informacji o zbliżających się zagrożeniach dla danej infrastruktury.

(3) **CIWIN byłby wielopoziomowym systemem komunikacji/ ostrzegania pełniącym dwie różne funkcje:** a) systemu wczesnego ostrzegania (SWO) łączącego Państwa Członkowskie z Komisją oraz b) forum wymiany koncepcji dotyczących OIK i najlepszych praktyk w celu udzielania wsparcia właścicielom i operatorom IK, złożonego z sieci specjalistów i posiadającego elektroniczny portal wymiany danych.

Niezależnie od wybranej opcji CIWIN uzupełniałby istniejące sieci; zostałyby podjęte konieczne kroki w celu uniknięcia powielania działań. Na dłuższą metę CIWIN byłby powiązany ze wszystkimi odpowiednimi właścicielami i operatorami IK w każdym Państwie Członkowskim poprzez np. KOK. Sygnały ostrzegawcze i najlepsze praktyki mogłyby być przekazywane za pośrednictwem tego organu, który jako jedyny byłby bezpośrednio połączony z Komisją i tym sposobem ze wszystkimi innymi Państwami Członkowskimi. Państwa Członkowskie mogłyby używać istniejących systemów informacyjnych w celu utworzenia krajowego CIWIN, łączącego władze z poszczególnymi właścicielami i operatorami. Ważne jest, aby te krajowe sieci mogły być używane przez odpowiednie organy OIK Państw Członkowskich oraz właścicieli i operatorów jako dwukierunkowy system komunikacji.

Przeprowadzi się badanie w celu ustalenia zakresu i specyfikacji technicznych koniecznych do utworzenia w przyszłości interfejsu CIWIN z Państwami Członkowskimi.

Pytania

Jaka formę powinien przybrać system CIWIN, aby móc udzielić wsparcia celom EPOIK?

Czy właściciele i operatorzy IK powinni być połączeni z CIWIN?

9.2. Wspólna metodologia

Różne Państwa Członkowskie mają różne poziomy ostrzegania odpowiadające różnym sytuacjom. W chwili obecnej nie istnieje sposób sprawdzenia, czy np. „wysoki" poziom zagrożenia w jednym Państwie Członkowskim oznacza to samo, co „wysoki" poziom zagrożenia w innym. Może to sprawiać, iż firmy międzynarodowe będą miały trudności w określeniu priorytetów w dziedzinie wydatków na środki ochronne. Próba dokonania harmonizacji różnych poziomów zagrożenia i nadania im odpowiedniej skali może zatem przynieść korzyści.

Dla każdego poziomu zagrożenia mógłby istnieć poziom gotowości. Tym sposobem zwykłe środki bezpieczeństwa mogą być wykorzystywane na zasadzie ogólnej, a w stosownych przypadkach zostaną użyte progresywne środki bezpieczeństwa. Państwo Członkowskie pragnące użyć danego środka mogłoby przeciwdziałać określonemu zagrożeniu poprzez użycie alternatywnych środków bezpieczeństwa.

Można by rozważyć utworzenie wspólnej metodologii w dziedzinie określania i klasyfikacji zagrożeń, zdolności, ryzyka, podatności na zagrożenia oraz w dziedzinie wyciągania wniosków dotyczących możliwości, prawdopodobieństwa oraz stopnia oddziaływania danego zagrożenia w zakresie zakłócenia funkcjonowania urządzeń infrastruktury. Obejmowałaby by ona klasyfikację ryzyka i wyznaczanie priorytetów, dzięki którym wydarzenia niosące ryzyko mogłyby być określane z perspektywy prawdopodobieństwa wystąpienia, wpływu oraz związku z innymi dziedzinami i procesami dotyczącymi ryzyka.

Pytania

W jakim stopniu harmonizacja lub wyskalowanie różnych poziomów ostrzegania byłaby pożądana i wykonalna?

Czy powinno się opracować wspólną metodologię określania i klasyfikacji zagrożeń, zdolności, ryzyka, podatności na zagrożenia oraz wyciągania wniosków dotyczących możliwości, prawdopodobieństwa oraz stopnia oddziaływania danego zagrożenia?

9.3. Finansowanie

W następstwie inicjatywy Parlamentu Europejskiego (utworzenie nowej pozycji budżetowej – projekt pilotażowy pt. „Walka z terroryzmem" – w budżecie na 2005 r.) w dniu 15 września Komisja podjęła decyzję o przyznaniu 7 mln EUR na finansowanie szeregu działań mających usprawnić europejskie systemy zapobiegania atakom terrorystycznym, gotowości i reakcji, w tym zarządzanie skutkami, ochronę infrastruktury krytycznej, badania nad finansowaniem terroryzmu, materiałami wybuchowymi i gwałtowną radykalizacją postaw. Ponad dwie trzecie tej kwoty jest przeznaczone na przygotowanie przyszłego Europejskiego Programu Ochrony Infrastruktury Krytycznej, integrację i rozwój zdolności wymaganych do zarządzania sytuacjami kryzysowymi o charakterze ponadnarodowym wynikającymi z możliwych ataków terrorystycznych i na środki wyjątkowe, które mogą być potrzebne, aby zapobiec znacznemu zagrożeniu lub wystąpieniu ataku. Oczekuje się, że finansowanie to będzie kontynuowane w 2006 r.

W okresie od 2007 do 2013 roku finansowanie przejmie program ramowy na rzecz bezpieczeństwa i ochrony swobód. Obejmuje on specjalny program dotyczący „zapobiegania aktom terrorystycznym, gotowości i zarządzania skutkami"; we wniosku Komisji przyznaje się kwotę 137,4 mln EUR na określenie istotnych potrzeb i opracowanie wspólnych norm technicznych w celu ochrony infrastruktury krytycznej.

Program udzieli finansowania wspólnotowego projektom dotyczącym ochrony infrastruktury krytycznej przedstawionym przez władze krajowe, regionalne i lokalne. Program skupia się na określeniu potrzeb związanych z ochroną i na udzielaniu informacji w celu opracowania wspólnych norm i dokonania oceny zagrożenia i ryzyka, tak aby chronić infrastrukturę krytyczną lub sporządzić szczególne plany działań w sytuacjach zagrożenia. Komisja korzystałaby z istniejącej wiedzy specjalistycznej lub pomagałaby w finansowaniu badań dotyczących współzależności w poszczególnych sektorach. Podnoszenie bezpieczeństwa infrastruktury zgodnie z ustalonymi potrzebami należy więc głównie do obowiązków Państw Członkowskich oraz właścicieli i operatorów. Sam program nie finansuje ulepszania ochrony infrastruktury krytycznej. Pożyczki od instytucji finansowych mogłyby zostać wykorzystane w celu podniesienia bezpieczeństwa infrastruktury w Państwach Członkowskich zgodnie z potrzebami określonymi w programie i w celu wdrożenia wspólnych norm. Komisja chętnie wesprze badania dotyczące poszczególnych sektorów, mające na celu ocenę skutków finansowych, jakie może mieć dla przemysłu podniesienie bezpieczeństwa infrastruktury.

Komisja finansuje projekty badawcze wspierające ochronę infrastruktury krytycznej poprzez działanie przygotowawcze na rzecz badań nad bezpieczeństwem[2] (2004-2006) i zaplanowała bardziej znaczące działania w dziedzinie badań nad bezpieczeństwem w swoim wniosku dotyczącym decyzji Rady i Parlamentu Europejskiego w sprawie siódmego programu ramowego badań (COM(2005)119 wersja ostateczna)[3] i w swoim wniosku dotyczącym decyzji Rady w sprawie szczególnego programu „współpraca" wdrażającego siódmy program ramowy (COM(2005)440 wersja ostateczna). Ukierunkowane badania mające na celu opracowanie praktycznych strategii lub narzędzi łagodzenia ryzyka mają kluczowe znaczenie dla zabezpieczenia krytycznej infrastruktury UE w perspektywie średnio- i długoterminowej. Wszystkie badania związane z bezpieczeństwem, w tym również w omawianej dziedzinie, zostaną poddane przeglądowi zasad etycznych w celu zapewnienia ich zgodności z Kartą Praw Podstawowych. Zapotrzebowanie na badania będzie jeszcze rosło w miarę wzrastania liczby jednostek infrastruktury.

Pytania

Jak oceniają Państwo koszt i wpływ wdrożenia proponowanych w niniejszej zielonej księdze środków w kontekście administracji i przemysłu? Czy uważają Państwo, że koszt ten jest proporcjonalny?

---

[2] Łączna kwota środków kredytowych w budżecie na lata 2004 i 2005 wyniosła 30 mln EUR. Komisja zaproponowała na 2006 r. kwotę 24 mln EUR, rozważaną obecnie przez władzę budżetową.

[3] Projekt budżetu Komisji przewiduje przeznaczenie kwoty 570 mln EUR na badania na rzecz bezpieczeństwa i przestrzeni kosmicznej w ramach siódmego programu ramowego badań i rozwoju technologicznego (RTD) (COM(2005)119 wersja ostateczna).

9.4. Ocena i kontrola

Ocena i kontrola realizacji EPOIK wydaje się wielopoziomowym procesem, wymagającym zaangażowania wszystkich zainteresowanych stron.

- **na poziomie UE można by ustanowić mechanizm wzajemnej oceny**, w ramach którego Państwa Członkowskie i Komisja pracowałyby razem nad oceną ogólnego poziomu realizacji EPOIK w każdym Państwie Członkowskim. Można by sporządzać roczne sprawozdania Komisji z postępów w dziedzinie realizacji EPOIK.

- **Komisja zdawałaby sprawozdanie z postępów Państwom Członkowskim i innym instytucjom w każdym roku kalendarzowym** w formie dokumentu roboczego służb Komisji.

- **Na poziomie Państw Członkowskich KOK mógłby nadzorować ogólną realizację EPOIK na obszarze właściwości każdego Państwa Członkowskiego, zapewniając zgodność z krajowym(-i) programem(-ami) OIK i programami OIK dla poszczególnych sektorów**, gwarantując ich skuteczne wdrażanie poprzez sporządzanie rocznych sprawozdań do Rady i Komisji.

Realizacja EPOIK byłaby dynamicznym procesem, bezustannie ewoluującym i ocenianym w celu dostosowywania programu do zmieniających się warunków i wyciągania wniosków ze zdobywanego doświadczenia. Wzajemna ocena i sprawozdania kontrolne Państw Członkowskich mogłyby zaliczać się do instrumentów służących do przeglądu EPOIK i stanowić możliwość składania propozycji nowych działań mających na celu wzmocnienie ochrony infrastruktury krytycznej.

Istotne informacje dotyczące EIK, pochodzące od Państw Członkowskich, mogłyby być udostępniane Komisji w celu opracowania oceny wspólnej podatności na zagrożenia, planów zarządzania skutkami, wspólnych norm ochrony IK, a także w celu nadania priorytetowego znaczenia działalności badawczej i w stosownych przypadkach regulacji i harmonizacji. Takie informacje byłyby zastrzeżone i miałyby charakter całkowicie poufny.

Komisja mogłaby kontrolować różne inicjatywy Państw Członkowskich, w tym te przewidujące finansowe skutki dla właścicieli i operatorów niezdolnych w określonym terminie do wznowienia niezbędnych usług świadczonych obywatelom.

Pytanie

Jakiego rodzaju mechanizmu oceny potrzebuje EPOIK? Czy wyżej wymieniony mechanizm byłby wystarczający?

Odpowiedzi należy przekazywać pocztą elektroniczną do dnia 15 stycznia 2006 r. na następujący adres e-mail: **JLS-EPCIP@cec.eu.int**. Ich treść będzie miała charakter poufny, chyba że udzielający odpowiedzi wyraźnie oświadczy, że chce ją upublicznić; w takim przypadku treść odpowiedzi zostanie zamieszczona na stronie internetowej Komisji.

ZAŁĄCZNIKI

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  - Environment (effect on the public and surrounding location);

  - Interdependency (between other critical infrastructure elements).

  - Political effects (confidence in the ability of government);

  - Psychological effects (may escalate otherwise minor events). both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

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.

Threat

Any indication, circumstance, or event with 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. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

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.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- Graduated security measures, which may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.