KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 27.10.2008
KOM(2008) 676 wersja ostateczna

2008/0200 (CNS)

Wniosek

DECYZJA RADY

w sprawie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN)

{SEC(2008) 2701}
{SEC(2008) 2702}

(przedstawiona przez Komisję)

UZASADNIENIE

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 w sprawie zapobiegania atakom terrorystycznym, gotowości i reagowania na nie oraz w „Programie solidarności UE w sprawie skutków zagrożeń i ataków terrorystycznych", przyjętych w grudniu 2004 r., Rada poparła plan Komisji zmierzający do przedstawienia europejskiego programu ochrony infrastruktury krytycznej (European Programme for Critical Infrastructure Protection – EPCIP) oraz wyraziła zgodę na utworzenie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (Critical Infrastructure Warning Information Network – CIWIN) przez Komisję.

W grudniu 2006 r. Komisja przedstawiła wniosek dotyczący dyrektywy w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony. Jednocześnie Komisja opublikowała komunikat w sprawie EPCIP. Wszystkie te dokumenty te określają założenia ochrony infrastruktury w UE. W komunikacie określono horyzontalne ramy ochrony infrastruktury krytycznej w UE oraz wyjaśniono, w jaki sposób program EPCIP (w tym sieć CIWIN) mogą zostać wprowadzone w życie.

Inicjatywa w sprawie CIWIN stanowi część programu EPCIP i obejmuje w szczególności proces wymiany informacji pomiędzy państwami członkowskimi UE oraz system informatyczny wspierający ten proces.

Kontekst ogólny

Bezpieczeństwo i gospodarka Unii Europejskiej, jak również dobrobyt jej mieszkańców, są uzależnione od określonej infrastruktury i zapewnianych z jej wykorzystaniem usług. Na przykład sieci telekomunikacyjne i energetyczne, usługi finansowe i systemy transportowe, usługi zdrowotne, a także zapewnienie bezpieczeństwa w zakresie wody pitnej i żywności mają zasadnicze znaczenie dla UE i jej państw członkowskich. Z jednej strony jakiekolwiek zniszczenie lub zakłócenie infrastruktury zapewniającej kluczowe usługi, a z drugiej niewłaściwa reakcja na tego rodzaju wydarzenie mogą doprowadzić do utraty życia, własności oraz załamania zaufania publicznego do UE. Skomplikowane współzależności oznaczają, że określone wydarzenie może wywołać efekt kaskadowy, przenoszący zagrożenie na inne sektory i dziedziny życia, które nie są ze sobą bezpośrednio i w oczywisty sposób powiązane. Ten rodzaj wzajemnych powiązań nie został odpowiednio dobrze zbadany, czego wynikiem może być niedostateczna ochrona infrastruktury krytycznej i niewystarczający poziom bezpieczeństwa dla obywateli UE.

Infrastruktura krytyczna w Unii Europejskiej podlega obecnie licznym i zróżnicowanym obowiązkom i środkom ochronnym, przy jednoczesnym braku minimalnych standardów o charakterze horyzontalnym. Niektóre państwa członkowskie osiągnęły już duży postęp w

określaniu własnej krajowej infrastruktury krytycznej, podjęły zdecydowane działania ochronne oraz dysponują różnorodnymi praktykami i strukturami w celu zapewnienia ochrony tej infrastruktury. Inne dopiero rozpoczynają ten proces i mogą czerpać duże korzyści z dostępu do najlepszych praktyk, takich jak metodologia oceny ryzyka. Problem może zostać określić w kategoriach geograficznych (tj. między państwami członkowskimi) oraz sektorowych (tj. między różnymi sektorami ochrony infrastruktury krytycznej).

Rozwiązanie kwestii wymiany informacji między państwami członkowskimi jest obszarem niezwykle skomplikowanym, który wymaga dobrze przemyślanego podejścia. Ważne jest, aby zapobiec powielaniu działań wynikającemu z niewystarczającej ilości informacji na temat podobnych sytuacji w innych państwach członkowskich: na przykład informacje dotyczące najlepszej praktyki w jednym państwie członkowskim mogą pomóc uniknąć kosztów ponownego opracowywania podobnej praktyki w innych państwach.

Ponadto istnieje obawa przed wymianą informacji szczególnie chronionych między zainteresowanymi stronami. Aby wymiana informacji była efektywna, należy stworzyć środowisko oparte na zaufaniu i elastyczności.

Obowiązujące przepisy w dziedzinie, której dotyczy wniosek

W Unii Europejskiej nie obowiązują obecnie żadne przepisy w zakresie wymiany informacji i ostrzeżeń w dziedzinie ochrony infrastruktury krytycznej, jednakże w 2006 r. Komisja przedstawiła wniosek dotyczący dyrektywy w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony (COM(2006) 787 wersja ostateczna). Jednocześnie Komisja opublikowała komunikat w sprawie EPCIP (COM(2006) 786 wersja ostateczna). W czerwcu 2008 r. Rada osiągnęła polityczne porozumienie odnośnie do wyżej wymienionej dyrektywy, zaś jej przyjęcie zaplanowano na drugą połowę 2008 r.

Ponadto w UE istnieje wiele sektorowych systemów wczesnego ostrzegania. Główną różnicą pomiędzy siecią CIWIN i istniejącymi systemami wczesnego ostrzegania jest międzysektorowy charakter tej pierwszej. Obecnie żaden z systemów wczesnego ostrzegania nie zapewnia takiej funkcjonalności o charakterze horyzontalnym i międzysektorowym, która byłaby dostępna dla szerszego grona zainteresowanych podmiotów (odpowiednich krajowych agencji i ministerstw odpowiedzialnych za ochronę infrastruktury krytycznej itp.) niż tylko służby ratownicze:

– decyzja Rady ustanawiająca wspólnotowy mechanizm ochrony ludności (przekształcenie) (2007/779/WE, Euratom);

– decyzja Rady w sprawie wspólnotowych warunków wczesnej wymiany informacji w przypadku zdarzenia radiacyjnego, ustanawiająca wspólnotowy system wczesnego powiadamiania i wymiany informacji w sytuacjach zagrożenia radiacyjnego (87/600/Euratom);

– dyrektywa Rady 82/894/EWG z dnia 21 grudnia 1982 r. w sprawie zgłaszania chorób zwierząt we Wspólnocie (82/894/EWG);

– dyrektywa Rady w sprawie środków ochronnych przed wprowadzaniem do Wspólnoty organizmów szkodliwych dla roślin (2000/29/WE);

– decyzja Parlamentu Europejskiego i Rady ustanawiająca sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie (2119/98/WE);

– dyrektywa Parlamentu Europejskiego i Rady w sprawie ogólnego bezpieczeństwa produktów (2001/95/WE);

– rozporządzenie (WE) Parlamentu Europejskiego i Rady ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (178/2002);

– decyzja Komisji dotycząca opracowania zintegrowanego skomputeryzowanego systemu weterynaryjnego pod nazwą Traces (2003/623/WE);

– decyzja Komisji zmieniająca regulamin wewnętrzny Komisji (2006/25/WE, Euratom).

Spójność z pozostałymi obszarami polityk i celami Unii

Niniejszy wniosek jest całkowicie zgodny z celami Unii Europejskiej, 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”.

Jest on także spójny z polityką w innych dziedzinach, gdyż jego celem nie jest zastępowanie istniejących środków, lecz ich uzupełnienie w celu lepszej ochrony europejskiej infrastruktury krytycznej.

KONSULTACJE Z ZAINTERESOWANYMI STRONAMI ORAZ OCENA SKUTKÓW

Konsultacje z zainteresowanymi stronami

Metody konsultacji, główne sektory objęte konsultacjami i ogólny profil respondentów

W trakcie i w ramach konsultacji w sprawie EPCIP przeprowadzono konsultacje w sprawie CIWIN ze wszystkimi zainteresowanymi stronami. Płaszczyzną konsultacji były:

– zielona księga w sprawie EPCIP, przyjęta 17 listopada 2005 r., z okresem konsultacji do 15 stycznia 2006 r. Swoje oficjalne odpowiedzi przesłały 22 państwa członkowskie. Uwagi zgłosiło także około 100 przedstawicieli sektora prywatnego. W opiniach tych wyrażano przeważnie poparcie dla idei stworzenia sieci CIWIN.

– szereg nieformalnych spotkań z udziałem przedstawicieli punktów kontaktowych z państw członkowskich zajmujących się ochroną infrastruktury krytycznej zorganizowanych przez Komisję (grudzień 2005 r., luty 2006 r., grudzień 2006 r., listopad 2007 r., luty 2008 marzec 2008 r.);

– badanie w sprawie stworzenia sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN), zakończone w styczniu 2008 r. przez zewnętrznego wykonawcę: Unisys. Jako część badania wykonawca przeprowadził rozmowy w sprawie CIWIN we wszystkich 27 państwach członkowskich;

– nieformalne spotkania z przedstawicielami sektora prywatnego. Zorganizowano liczne nieformalne spotkania zarówno z przedstawicielami indywidualnych przedsiębiorstw, jak również z przedstawicielami stowarzyszeń branżowych.

Streszczenie odpowiedzi oraz sposób ich uwzględnienia

Mimo że zielona księga w sprawie EPCIP miała szerszy zakres i obejmowała konsultacje z zainteresowanymi stronami w odniesieniu do wielu aspektów tego programu (np. cel i kluczowe zasady EPCIP, etapy wdrażania itd.), częściowo dotyczyła również CIWIN.

Uwagi dotyczące zielonej księgi w sprawie EPCIP oraz dyskusje prowadzone ze wszystkimi zainteresowanymi stronami miały duży wpływ na kształt wniosku w sprawie CIWIN. Początkowo państwa członkowskie nie miały jednakowych poglądów na stworzenie CIWIN. Niektóre z nich opowiadały się za wielopoziomowym systemem komunikacyjno-ostrzegawczym pełniącym dwie różne funkcje: systemem wczesnego ostrzegania oraz elektronicznego forum wymiany pomysłów i najlepszych praktyk dotyczących ochrony infrastruktury krytycznej. Szereg państw członkowskich popierało jednak ograniczenie roli CIWIN albo do funkcji forum, albo systemu wczesnego ostrzegania stanowiącego łącznik między państwami członkowskimi a Komisją. Podczas konsultacji dwa państwa członkowskie były przeciwne sieci CIWIN. Z uwagi na zróżnicowane poglądy kwestia ta została poddana dyskusji z państwami członkowskimi podczas regularnych spotkań z udziałem przedstawicieli punktów kontaktowych ds. ochrony infrastruktury krytycznej. Wynikiem tych dyskusji jest ostateczna koncepcja CIWIN.

Gromadzenie i wykorzystanie wiedzy specjalistycznej

Dziedziny nauki i wiedzy specjalistycznej, których dotyczy wniosek

Wiedzę specjalistyczną gromadzono zarówno w trakcie licznych spotkań i seminariów przeprowadzonych w 2006, 2007 i 2008 r., jak również w procesie konsultacji zielonej księgi w sprawie EPCIP. Informacje pochodziły od wszystkich stron zainteresowanych omawianą kwestią.

Zastosowana metodologia

W marcu 2006 r. Komisja udzieliła zamówienia na opracowanie studium wykonalności CIWIN w celu zebrania informacji na temat najlepszych praktyk w zakresie ochrony infrastruktury krytycznej oraz przeprowadzenia rozmów z ekspertami w państwach członkowskich na temat wymogów sieci CIWIN, zarówno jako sieci wymiany informacji, jak i systemu wczesnego ostrzegania, z uwzględnieniem istniejących infrastruktur i sieci na poziomie krajowym i międzynarodowym.

Kolejnym celem było stworzenie wspólnej platformy wymiany informacji istotnych dla ochrony infrastruktury krytycznej.

Główne organizacje/eksperci, z którym przeprowadzono konsultacje

Wszystkie państwa członkowskie UE.

Streszczenie otrzymanych i wykorzystanych opinii

Nie stwierdzono istnienia potencjalnie poważnych zagrożeń o nieodwracalnych skutkach.

Sposoby udostępnienia opinii ekspertów

Załączniki do oceny skutków.

Ocena skutków

Porozumienie w sprawie przyjęcia oddzielnego wniosku dotyczącego sieci CIWIN osiągnięto już w ramach pakietu EPCIP, a dokładniej w komunikacie Komisji w sprawie EPCIP. W ocenie skutków przewidziano pięć wariantów strategicznych:

Wariant 1: Wariant zachowania *status quo*. Zgodnie z tym wariantem nie podjęto by żadnych działań przekrojowych na poziomie europejskim a państwa członkowskie zajmowałyby się rozwiązaniem problemu we własnym zakresie.

Wariant 2: Sieć CIWIN jako rozszerzenie istniejących systemów wczesnego ostrzegania. Zgodnie z tym wariantem (który wymagałby zarówno funkcjonalnego przeglądu istniejącej architektury informatycznej, jak i zmiany jej podstaw prawnych) rolą CIWIN byłoby zapewnienie interoperacyjności istniejących systemów wczesnego ostrzegania oraz udostępnienie ich różnym służbom w ramach UE oraz w ministerstwach państw członkowskich. W związku z tym, że wariant ten obejmowałby wyłącznie funkcję wczesnego ostrzegania, jakikolwiek krok w kierunku dołączenia platformy wymiany informacji i najlepszych praktyk wymagałby znaczącego i kosztownego przeglądu istniejących systemów wczesnego ostrzegania.

Wariant 3: Sieć CIWIN jako otwarta platforma (niezabezpieczonej) wymiany informacji związanych z ochroną infrastruktury krytycznej. Wariant ten będzie wymagał opracowania narzędzia informatycznego, które będzie dostępne dla nieograniczonego grona użytkowników i będzie funkcjonowało jako zwykła strona internetowa. Bez wątpienia pomogłoby to poprawianiu świadomości w zakresie ochrony infrastruktury krytycznej w Europie i zwiększyłoby bezpośrednią wymianę informacji między podmiotami zainteresowanymi. Niemniej jednak, ponieważ właściciel jakichkolwiek informacji zamieszczonych na stronie nigdy nie wiedziałby, kto jest ich użytkownikiem ostatecznym, ilość informacji udostępnianych w systemie byłaby znacznie ograniczona.

Wariant 4: CIWIN jako zabezpieczony dobrowolny wielopoziomowy system komunikacyjno-ostrzegawczy pełniący dwie różne funkcje: systemu wczesnego ostrzegania i elektronicznego forum wymiany pomysłów i najlepszych praktyk dotyczących ochrony infrastruktury krytycznej. W tym wariancie CIWIN zostałby utworzony jako narzędzie informatyczne przeznaczone do przechowywania i przekazywania informacji szczególnie chronionych, oznaczonych klauzulą tajności „UE RESTREINT" lub niższą. System miałby dwie główne funkcje: (1) bezpiecznego forum w celu wymiany informacji, z dużym naciskiem na wymianę najlepszych praktyk, dialog i budowanie zaufania na poziomie UE; (2) systemu wczesnego ostrzegania w zakresie infrastruktury krytycznej. Państwa członkowskie mogłyby zgodnie ze swym wyborem korzystać z całego systemu, wybrać niektóre z oferowanych funkcji lub wcale nie używać systemu.

Wariant 5: CIWIN jako obowiązkowy wielopoziomowy system komunikacyjno-ostrzegawczy pełniący dwie różne funkcje: systemu wczesnego ostrzegania i elektronicznego forum wymiany pomysłów i najlepszych praktyk dotyczących ochrony infrastruktury krytycznej. Zgodnie z tym wariantem CIWIN byłby systemem obowiązkowym, do którego każde

państwo członkowskie musiałoby wprowadzać i aktualizować regularnie wszystkie istotne informacje.

Komisja przeprowadziła ocenę skutków wymienioną w programie prac. Wariant 4 – CIWIN jako zabezpieczony dobrowolny (z możliwością przystąpienia) wielopoziomowy system komunikacyjno-ostrzegawczy pełniący dwie różne funkcje: systemem wczesnego ostrzegania oraz forum elektronicznym w celu wymiany pomysłów i najlepszych praktyk w zakresie ochrony infrastruktury krytycznej – wyraźnie prezentuje najkorzystniejszy stosunek zalet i wad. Zgodnie z tym wariantem CIWIN stanowiłby bezpieczne środowisko wymiany informacji, przyczyniłby się w dużej mierze do budowania zaufania pomiędzy zainteresowanymi podmiotami oraz umożliwiłby wymianę ostrzeżeń.

Ocenę skutków CIWIN załączono do niniejszego wniosku.

ASPEKTY PRAWNE WNIOSKU

Krótki opis proponowanych działań

Celem proponowanych działań jest wsparcie państw członkowskich w wymianie informacji na temat wspólnych zagrożeń, podatności na zagrożenia oraz odpowiednich środków i strategii zmniejszających ryzyko w celu ochrony infrastruktury krytycznej.

Podstawa prawna

Podstawą prawną wniosku są art. 308 Traktatu ustanawiającego Wspólnotę Europejską oraz art. 203 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej.

Zasada pomocniczości

Zasada pomocniczości ma zastosowanie, o ile wniosek nie podlega wyłącznym kompetencjom Wspólnoty.

Cele wniosku nie mogą być osiągnięte w sposób wystarczający przez państwa członkowskie z następujących względów.

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.

Wprawdzie każde państwo członkowskie samo odpowiada za ochronę infrastruktury krytycznej na własnym terytorium, ale transgraniczną platformę obejmującą całą UE w celu zapewnienia dostępności informacji dla wszystkich państw członkowskich, które mogą z nich skorzystać, z pewnością można wprowadzić wyłącznie na poziomie UE.

Działanie Wspólnoty zapewni lepsze osiągnięcie celów wniosku z następujących względów.

Żadne państwo członkowskie nie jest w stanie samo zapewnić ogólnoeuropejskiej wymiany informacji lub wymiany szybkich ostrzeżeń. Oczywiste jest zatem, że działanie na poziomie UE niesie dodatkową korzyść w postaci skoordynowania tych informacji, które być może są już dostępne, ale jeszcze nie są dzielone z innymi.

Wyłącznie podejście europejskie może zagwarantować, że państwa członkowskie zamierzające dzielić się informacjami i otrzymywać je będą jednakowo traktowane, że żadne z państw członkowskich nie będzie dyskryminowane podczas współpracy ze względu na położenie geograficzne oraz że informacje rzeczywiście dotrą do tych, którzy chcą je otrzymać.

Istnieje bezpośredni związek między interdyscyplinarną współpracą europejską a bezpieczeństwem narodowym. W dzisiejszym świecie współzależności transgranicznych, zarówno na płaszczyźnie geograficznej, jak i międzysektorowej, jedne państwa członkowskie mogą oferować usługi innym państwom członkowskim lub mogą mieć wpływ na świadczenie usług w innych państwach członkowskich. Istnieje zatem ryzyko, że jedno państwo członkowskie poniesie szkodę wskutek braku właściwej ochrony infrastruktury na terytorium innego państwa członkowskiego.

Coraz większa liczba infrastruktur ma wymiar europejski, co oznacza, że wyłącznie krajowe podejście nie jest wystarczające. Istnieje wyraźna potrzeba sprostania różnorodnym zagrożeniom, które mogą wpłynąć na europejską infrastrukturę krytyczną.

Wniosek jest zatem zgodny z zasadą pomocniczości.

Zasada proporcjonalności

Wniosek jest zgodny z zasadą proporcjonalności z następujących względów.

Niniejszy wniosek nie wykracza poza to, co jest konieczne do osiągnięcia jego głównego celu, czyli współpracy państw członkowskim w dziedzinie, której wniosek dotyczy, w szczególności z uwzględnieniem gotowości państw członkowskich do uczestnictwa. Zaproponowane działanie pozwala państwom członkowskim, które nie chcą uczestniczyć w CIWIN, na wycofanie się z systemu.

W porównaniu z korzyściami które przyniesie, CIWIN nie będzie miał znaczącego bezpośredniego wpływu finansowego ani na budżety państw członkowskich, ani na budżet UE. Na przykład koszty utrzymania wyniosłyby w przybliżeniu 550 000 euro rocznie, podczas gdy koszty zdarzeń, którym CIWIN może potencjalnie zapobiec lub których skutki może ograniczyć, są znacznie wyższe.

Wybór instrumentów

Proponowane instrumenty: decyzja Rady.

Inne instrumenty byłyby niewłaściwe z następujących względów:

Aby prototyp CIWIN stał się w pełni funkcjonalny i dostępny dla wszystkich państw członkowskich UE, konieczna jest podstawa prawna. Z uwagi na fakt, że przedmiot, którego dotyczy ten instrument prawny, ma zakres szczegółowy, a nie ogólny, decyzja Rady pozwoli najlepiej osiągnąć jego cel, a jednocześnie będzie zobowiązywać użytkowników systemu (państwa członkowskie i Komisję) do przestrzegania ewentualnej poufności wymienianych danych.

WPŁYW NA BUDŻET

Wpływ proponowanej regulacji na budżet przedstawiono w załączonej do niniejszego wniosku ocenie skutków finansowych. Program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa” na lata 2007–2013 przyczyni się do wdrożenia niniejszej decyzji.

INFORMACJE DODATKOWE

Symulacja, faza pilotażowa i okres przejściowy

Symulacja i faza pilotażowa wniosku zostały lub zostaną przeprowadzone.

Klauzula przeglądu/rewizji/wygaśnięcia

Wniosek zawiera klauzulę przeglądu.

Wniosek zawiera klauzulę rewizji.

2008/0200 (CNS)

Wniosek

DECYZJA RADY

w sprawie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN)

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],

a także mając na uwadze, co następuje:

(1) W konkluzjach Rady w sprawie zapobiegania atakom terrorystycznym, gotowości i reagowania na nie oraz w „Programie solidarności UE w sprawie skutków zagrożeń i ataków terrorystycznych", przyjętych w grudniu 2004 r., Rada poparła plan Komisji zmierzający do przedstawienia europejskiego programu ochrony infrastruktury krytycznej oraz wyraziła zgodę na utworzenie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej przez Komisję[3]..

(2) W listopadzie 2005 r. Komisja przyjęła zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej (EPCIP), w której opisano warianty strategiczne, jakie Komisja mogłaby zastosować przy opracowywaniu EPCIP i CIWIN. Wyniki konsultacji nad zieloną księgą potwierdziły zainteresowanie większości państw członkowskich stworzeniem CIWIN.

(3) W grudniu 2006 r. Komisja przyjęła komunikat w sprawie EPCIP[4], w którym zapowiedziała, że CIWIN zostanie stworzony w drodze oddzielnego wniosku Komisji i zapewni platformę do bezpiecznej wymiany najlepszych praktyk.

(4) Kilka wydarzeń dotyczących infrastruktury krytycznej w Europie, takich jak ogólnoeuropejska awaria sieci energetycznej w 2006 r., dowiodło, że konieczna jest lepsza i bardziej efektywna wymiana informacji, aby zapobiec takim sytuacjom lub ograniczyć ich zakres.

---

1 Dz.U. C […] z […], s. […].
2 Dz.U. C […] z […], s. […].
3 14894/04.
4 COM(2006) 786 wersja ostateczna.

(5) Należy stworzyć system informacyjny, który umożliwi państwom członkowskim i Komisji wymianę informacji i ostrzeżeń w zakresie ochrony infrastruktury krytycznej oraz ożywi dialog pomiędzy nimi na ten temat, a także przyczyni się do poprawy integracji i lepszej koordynacji krajowych programów badań nad ochroną infrastruktury krytycznej, które są rozproszone i podzielone.

(6) CIWIN przyczyni się do polepszenia ochrony infrastruktury krytycznej w UE przez udostępnienie systemu informacji, który umożliwi współpracę państw członkowskich; zaproponuje również wydajną i szybką alternatywę dla czasochłonnych metod poszukiwania informacji na temat infrastruktury krytycznej we Wspólnocie.

(7) CIWIN powinien w szczególności pobudzić opracowywanie odpowiednich środków, mających na celu ułatwienie wymiany najlepszych praktyk, a także służyć jako narzędzie do przekazywania ostrzeżeń oraz informacji o zbliżających się zagrożeniach w bezpieczny sposób.

(8) CIWIN powinien zapewnić unikanie powielania i powinien uwzględniać szczególne cechy charakterystyczne, wiedzę specjalistyczną, porozumienia i zakres kompetencji każdego z istniejących sektorowych systemów wczesnego ostrzegania.

(9) Na przestrzeni lat Komisja wypracowała operacyjną zdolność udzielania wsparcia w reagowaniu na szeroki wachlarz sytuacji kryzysowych przez różnorodne systemy wczesnego ostrzegania, które są dostosowane do poszczególnych sektorów oraz ukierunkowane na specjalistyczne usługi w ramach UE. Niemniej jednak istniejące systemy wczesnego ostrzegania nie zapewniają funkcjonalności ochrony infrastruktury krytycznej, która byłaby dostępna dla grona zainteresowanych podmiotów szerszego niż właściwe organy w danym sektorze i służby ratownicze.

(10) Współzależność pomiędzy infrastrukturą krytyczną w państwach członkowskich oraz różnorodne poziomy ochrony tej infrastruktury w państwach członkowskich pozwalają zakładać, że stworzenie wspólnotowego narzędzia do wymiany informacji i ostrzeżeń dotyczących ochrony infrastruktury krytycznej o charakterze horyzontalnym i międzysektorowym zwiększyłoby bezpieczeństwo obywateli.

(11) Uwzględniając przyszłą dostępność transeuropejskiej telematycznej sieci komunikacyjnej między organami administracji (S-TESTA) lub jakiejkolwiek alternatywnej zabezpieczonej sieci zarządzanej przez Komisję, Komisja powinna wybrać najbardziej odpowiednią platformę technologiczną dla CIWIN i zobowiązać użytkowników końcowych do spełnienia wymogów technicznych przez nią nałożonych.

(12) Proces wymiany informacji na temat ochrony infrastruktury krytycznej między zainteresowanymi podmiotami wymaga relacji opartych na zaufaniu, tak aby informacje zastrzeżone lub informacje szczególnie chronione, które zostały dobrowolnie udostępnione, nie zostały publicznie ujawnione oraz aby dane szczególnie chronione były odpowiednio zabezpieczone.

(13) Dostęp do CIWIN powinien być ograniczony tylko do upoważnionych użytkowników zgodnie z uzgodnionymi warunkami, procedurami i środkami bezpieczeństwa. W państwach członkowskich użytkownikami sieci powinny być wyłącznie właściwe

organy krajowe, zaś w ramach Komisji dostęp powinien być ograniczony do właściwych służb.

(14) Jakiekolwiek koszty wynikające z działalności CIWIN na szczeblu wspólnotowym powinny być pokrywane ze środków wspólnotowych lub stosownych programów wspólnotowych.

(15) Jakiekolwiek koszty wynikające z działalności CIWIN na szczeblu krajowym powinny finansować same państwa członkowskie, chyba że zapadną inne postanowienia na poziomie wspólnotowym.

(16) W związku z tym, że cel zamierzonego działania, a mianowicie bezpieczna i szybka wymiana informacji między państwami członkowskimi, nie może być osiągnięty w sposób wystarczający przez państwa członkowskie, może zaś być lepiej osiągnięty na szczeblu wspólnotowym ze względu na skutki przewidywanych działań, Wspólnota może podjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsza decyzja nie wykracza poza to, co jest konieczne do osiągnięcia wyżej wymienionego celu.

(17) Niniejsza decyzja nie narusza podstawowych praw i przestrzega zasad uznanych w szczególności w Karcie praw podstawowych Unii Europejskiej,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1
Przedmiot

Niniejsza decyzja ustanawia bezpieczny system wymiany informacji, komunikacji i ostrzeżeń – sieć ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN) – w celu wspierania państw członkowskich w wymianie informacji na temat wspólnych zagrożeń, podatności na zagrożenia oraz odpowiednich środków i strategii zmniejszających ryzyko związane z ochroną infrastruktury krytycznej.

Artykuł 2
Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

„Infrastruktura krytyczna” oznacza te zasoby, systemy lub ich części znajdujące się na terytorium państw członkowskich, które są niezbędne do utrzymania podstawowych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu gospodarczego lub społecznego mieszkańców, których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku braku zachowania tych funkcji.

„Uczestniczące państwo członkowskie” oznacza to państwo członkowskie, które podpisało protokół ustaleń z Komisją.

„Organ Wykonawczy CIWIN” oznacza punkt kontaktowy CIWIN w danym państwie członkowskim lub w Komisji, który zapewnia właściwe wykorzystanie CIWIN i zgodność z wytycznymi dla użytkowników w obrębie danego państwa członkowskiego lub Komisji.

„Zagrożenie" oznacza czynnik, okoliczność lub zdarzenie, które może spowodować zakłócenie lub zniszczenie infrastruktury krytycznej lub jej elementu.

Artykuł 3
Uczestnictwo

W sieci CIWIN może uczestniczyć i może z niej skorzystać każde państwo członkowskie. Uczestnictwo w CIWIN jest uzależnione od podpisania protokołu ustaleń, zawierającego wymogi techniczne i wymogi bezpieczeństwa stosowane w odniesieniu do CIWIN, a także informacje na temat miejsc, które mają zostać połączone z CIWIN.

Artykuł 4
Funkcje

(1) CIWIN spełnia następujące dwie funkcje:

(a) elektronicznego forum wymiany informacji dotyczących ochrony infrastruktury krytycznej;

(b) systemu wczesnego ostrzegania, który umożliwia uczestniczącym państwom członkowskim i Komisji wysyłanie ostrzeżeń o zbliżającym się ryzyku i zagrożeniach dla infrastruktury krytycznej.

(2) Elektroniczne forum obejmuje obszary stałe i obszary dynamiczne.

Obszary stałe włącza się do systemu na stałe. Mimo że ich zawartość może podlegać zmianom, obszarów tych nie można usunąć, zmienić ich nazwy ani dodać nowych. Załącznik I zawiera listę obszarów stałych.

Obszary dynamiczne tworzy się na żądanie i służą one określonemu celowi. Są one usuwane po zrealizowaniu swojej pierwotnej funkcji. Załącznik II zawiera listę obszarów dynamicznych, które zostaną stworzone po utworzeniu CIWIN.

Artykuł 5
Rola państw członkowskich

(1) Uczestniczące państwa członkowskie wyznaczają Organ Wykonawczy CIWIN i informują Komisję o tym fakcie. Organ Wykonawczy CIWIN odpowiada za udzielanie lub odmowę przyznania prawa dostępu do CIWIN w obrębie danego państwa członkowskiego.

(2) Uczestniczące państwa członkowskie zapewniają dostęp do CIWIN zgodnie z wytycznymi przyjętymi przez Komisję.

(3) Uczestniczące państwa członkowskie udostępniają i regularnie aktualizują informacje na temat ochrony infrastruktury technicznej istotne z punktu widzenia wspólnego interesu UE.

Artykuł 6
Rola Komisji

(1) Komisja odpowiada za:

(a) rozwój techniczny i zarządzanie CIWIN, w tym jego strukturę informatyczną oraz elementy służące wymianie informacji;

(b) ustanawianie wytycznych dotyczących warunków korzystania z systemu, obejmujących poufność, przekazywanie, przechowywanie, archiwizowanie i usuwanie informacji. Komisja ustala również warunki i procedury przyznawania pełnego lub ograniczonego dostępu do CIWIN.

(2) Komisja powołuje Organ Wykonawczy CIWIN, który odpowiada za udzielanie lub odmowę przyznania praw dostępu do CIWIN w Komisji.

(3) Komisja udostępnia i regularnie aktualizuje informacje na temat ochrony infrastruktury krytycznej istotne z punktu widzenia wspólnego interesu UE.

Artykuł 7
Bezpieczeństwo

(1) CIWIN ustanawia się jako bezpieczny system przystosowany do przetwarzania informacji oznaczonych klauzulą tajności „RESTREINT UE" lub niższą.

Komisja wybiera najbardziej odpowiednią platformę technologiczną sieci CIWIN, zaś użytkownicy są zobowiązani do spełnienia wymogów technicznych nałożonych przez Komisję.

Poziom bezpieczeństwa sieci CIWIN aktualizuje się w miarę potrzeby.

(2) Prawa użytkowników do dostępu do dokumentów są oparte na zasadzie „ścisłej potrzeby", zaś szczegółowe instrukcje autora odnośnie do ochrony i przekazywania danego dokumentu muszą być ściśle przestrzegane.

(3) Państwa członkowskie i Komisja podejmują niezbędne środki bezpieczeństwa, aby:

(a) uniemożliwić osobie nieupoważnionej uzyskanie dostępu do CIWIN;

(b) zagwarantować, że podczas korzystania z CIWIN upoważnione osoby mają dostęp wyłącznie do tych danych, które są w zakresie ich kompetencji;

(c) uniemożliwić czytanie, kopiowanie, modyfikowanie lub usuwanie informacji przez osoby nieupoważnione.

(4) Zamieszczanie informacji w CIWIN nie ma wpływu na własność tych informacji. Upoważnieni użytkownicy ponoszą wyłączną odpowiedzialność za udostępniane przez nich informacje oraz są zobowiązani zapewnić ich pełną zgodność z istniejącymi przepisami prawa wspólnotowego i krajowego.

Artykuł 8
Wytyczne dla użytkowników

Komisja opracowuje i regularnie aktualizuje wytyczne dla użytkowników zawierające pełne dane dotyczące funkcji i roli CIWIN.

Artykuł 9
Koszty

Koszty ponoszone w związku z działalnością, utrzymywaniem i centralnymi funkcjami CIWIN są pokrywane z budżetu wspólnotowego. Koszty związane z dostępem do CIWIN użytkowników w obrębie uczestniczących państw członkowskich są ponoszone przez uczestniczące państwa członkowskie.

Artykuł 10
Przegląd

Raz na trzy lata Komisja dokonuje przeglądu i oceny działania CIWIN, a także przedkłada państwom członkowskim regularne sprawozdania.

Pierwsze sprawozdanie, które zostaje przedstawione w ciągu trzech lat po wejściu w życie niniejszej decyzji, określa w szczególności te elementy sieci wspólnotowej, które powinny zostać ulepszone lub dostosowane. Zawiera także wszelkie wnioski, które Komisja uzna za niezbędne w celu zmiany lub dostosowania niniejszej decyzji.

Artykuł 11
Data stosowania

Niniejszą decyzję stosuje się od 1 stycznia 2009 r.

Artykuł 12
Adresaci

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący

ZAŁĄCZNIK I

OBSZARY STAŁE CIWIN

Obszary stałe, o których mowa w art. 4, składają się z następujących elementów:

(1) obszary państw członkowskich, umożliwiające uczestniczącym państwom członkowskim stworzenie własnych obszarów na portalu CIWIN. Wyłączną odpowiedzialność za organizację, administrację i zawartość tego obszaru ponoszą państwa członkowskie; dostęp do tego obszaru będą mieli wyłącznie użytkownicy z danego państwa członkowskiego;

(2) obszary sektorowe, obejmujące 11 oddzielnych sektorów: przemysł chemiczny; energetykę; sektor finansowy; żywność; zdrowie; technologie informacyjne i komunikacyjne; sektor jądrowego cyklu paliwowego; obiekty badawcze, przestrzeń kosmiczną, transport i wodę. Powstanie również międzysektorowy podobszar obejmujący zagadnienia ogólne i kwestie istotne dla wielu sektorów;

(3) obszar Organu Wykonawczego CIWIN służący jako strategiczna platforma koordynacji i współpracy, mająca na celu propagowanie i usprawnianie działań i komunikacji w odniesieniu do ochrony infrastruktury krytycznej. Obszar ten będzie dostępny wyłącznie dla Organu Wykonawczego CIWIN;

(4) obszar zewnętrznej współpracy UE ukierunkowany na poprawianie świadomości w zakresie współpracy zewnętrznej dotyczącej ochrony infrastruktury krytycznej oraz w zakresie standardów ochrony infrastruktury krytycznej poza UE;

(5) katalog kontaktów umożliwiający wyszukiwanie danych kontaktowych innych użytkowników CIWIN lub specjalistów w zakresie ochrony infrastruktury krytycznej.

ZAŁĄCZNIK II

OBSZARY DYNAMICZNE CIWIN

Dynamiczne obszary, o których mowa w art. 4, obejmują następujące elementy:

(1) obszar grupy roboczej specjalistów zapewniających wsparcie grupom specjalistów ds. ochrony infrastruktury krytycznej;

(2) obszar projektów zawierający informacje na temat projektów finansowanych przez Komisję;

(3) obszary ostrzeżeń, które mogą zostać utworzone w wyniku wysłania ostrzeżenia przez system wczesnego ostrzegania i będą stanowić kanał komunikacyjny podczas działań związanych z ochroną infrastruktury krytycznej;

(4) obszar tematów specjalnych, skupiający się na szczególnych zagadnieniach.

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. TYTUŁ WNIOSKU:

Decyzja Rady w sprawie sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN).

2. STRUKTURA ABM/ABB

Działanie 18.05: Bezpieczeństwo i ochrona swobód

Cel 2: Ochrona infrastruktury krytycznej

3. POZYCJE W BUDŻECIE

3.1. Pozycje w budżecie (pozycje operacyjne oraz powiązane pozycje pomocy technicznej i administracyjnej (dawniej pozycje B..A)), wraz z treścią:

Pozycja w budżecie: 18.050800

Treść: Zapobieganie aktom terrorystycznym, gotowość i zarządzanie skutkami

3.2. Czas trwania działania i wpływu finansowego:

Od 2009 roku.

3.3. Informacje budżetowe:

Pozycja w budżecie	Rodzaj wydatków		Nowe	Wkład EFTA	Wkład krajów ubiegających się o członkowstwo	Dział w perspektywie finansowej
18.050800	Nieobowiązkowe	Zróżnicowane[5]	NIE	NIE	NIE	3A

[5] Środki zróżnicowane.

4. ZESTAWIENIE ZASOBÓW

4.1. Zasoby finansowe

4.1.1. Zestawienie środków na zobowiązania (CA) i środków na płatności (PA)

w mln EUR (do 3 miejsc po przecinku)

Rodzaj wydatków	Sekcja nr		2009 r.	2010 r.	2011 r.	2012 r.	2013 r.	Razem
Wydatki operacyjne[6]								
Środki na zobowiązania (CA)	8.1.	a	0,95	0,55	0,55	0,55	0,55	3,15
Środki na płatności (PA)		b	0,95	0,55	0,55	0,55	0,55	3,15
Wydatki administracyjne w ramach kwoty referencyjnej[7]								
Pomoc techniczna i administracyjna (NDA)	8.2.4.	c	nd.	nd.	nd.	nd.	nd.	nd.
KWOTA REFERENCYJNA OGÓŁEM								
Środki na zobowiązania		a+c	0,95	0,55	0,55	0,55	0,55	3,15
Środki na płatności		b+c	0,95	0,55	0,55	0,55	0,55	3,15
Wydatki administracyjne <u>nieuwzględnione</u> w kwocie referencyjnej[8]								
Wydatki na zasoby ludzkie i powiązane wydatki (NDA)	8.2.5.	d	0,117	0,117	0,117	0,117	0,117	0,585
Wydatki administracyjne, inne niż koszty zasobów ludzkich i powiązane koszty, nieuwzględnione w kwocie referencyjnej (NDA)	8.2.6.	e	0,015	0,015	0,015	0,015	0,015	0,075
Ogółem CA w tym koszty zasobów ludzkich		a+c+d+e	1,082	0,682	0,682	0,682	3,81	
Ogółem PA w tym koszty zasobów ludzkich		b+c+d+e	1,082	0,682	0,682	0,682	3,81	

6 Wydatki niewchodzące w zakres rozdziału xx 01 w tytule xx.

7 Wydatki w ramach art. xx 01 04 w tytule xx.

8 Wydatki w ramach rozdziału xx 01 z wyłączeniem art. xx 01 04 lub xx 01 05.

4.1.2. Zgodność z programowaniem finansowym

☒ Wniosek jest zgodny z obecnym programowaniem finansowym.

☐ Wniosek wymaga przeprogramowania odpowiedniego działu w perspektywie finansowej.

☐ Wniosek może wymagać zastosowania postanowień porozumienia międzyinstytucjonalnego (tzn. instrumentu elastyczności lub zmiany perspektywy finansowej)[9].

4.1.3. Wpływ finansowy na dochody

☒ Wniosek nie ma wpływu finansowego na dochody

☐ Wniosek ma następujący wpływ finansowy na dochody:

4.2. Zasoby ludzkie w przeliczeniu na etaty (w tym urzędnicy, pracownicy zatrudnieni na czas określony i personel zewnętrzny) – szczegółowe informacje w pkt 8.2.1.

Zapotrzebowania na dany rok	2009 r.	2010 r.	2011 r.	2012 r.	2013 r.
Zasoby ludzkie ogółem	1	1	1	1	1

5. OPIS I CELE

5.1. Potrzeba, która ma zostać zaspokojona w perspektywie krótko- lub długoterminowej

Celem szczegółowym CIWIN jest umożliwienie koordynacji i współpracy w zakresie informacji na temat ochrony infrastruktury krytycznej na szczeblu UE. Przede wszystkim powinien on zapewnić bezpieczną i ustrukturyzowaną wymianę informacji, a tym samym umożliwić użytkownikom szybkie i efektywne pozyskiwanie wiedzy o najlepszych praktykach w innych państwach członkowskich UE oraz umożliwić państwom członkowskim korzystanie z systemu wczesnego ostrzegania w zakresie ochrony infrastruktury krytycznej.

5.2. Wartość dodana z tytułu zaangażowania Wspólnoty i spójność wniosku z innymi instrumentami finansowymi oraz możliwa synergia

Chociaż każde państwo członkowskie samo odpowiada za ochronę infrastruktury krytycznej na własnym terytorium, to jednak transgraniczną platformę wymiany informacji obejmującą całą UE i zapewniającą dostępność informacji wszystkim państwom członkowskim, które mogą z nich skorzystać, z pewnością można wprowadzić wyłącznie na poziomie UE. Żadne państwo członkowskie nie jest w stanie samo zapewnić ogólnoeuropejskiej wymiany informacji lub wymiany szybkich ostrzeżeń. Oczywiste jest zatem, że działanie na poziomie UE niesie dodatkową korzyść w postaci skoordynowania tych informacji, które być może są

[9] Zob. pkt. 19 i 24 porozumienia międzyinstytucjonalnego.

już dostępne, ale jeszcze nie są dzielone z innymi. Wyłącznie podejście europejskie może zagwarantować, że państwa członkowskie zamierzające dzielić się informacjami i otrzymywać je są jednakowo traktowane, że żadne z państw członkowskich nie jest dyskryminowane podczas współpracy ze względu na położenie geograficzne, oraz że informacje rzeczywiście docierają do tych, którzy chcą je otrzymać.

5.3. Cele, spodziewane wyniki oraz wskaźniki związane z wnioskiem w kontekście ABM

Głównym celem CIWIN powinno być pobudzenie wypracowania odpowiednich środków mających na celu ułatwianie wymiany najlepszych praktyk, a także funkcjonowanie jako narzędzie do przekazywania ostrzeżeń oraz informacji o zbliżających się zagrożeniach w bezpieczny sposób. System powinien gwarantować, że odpowiednie osoby otrzymują właściwe informacje we właściwym czasie.

Stworzenie CIWIN zostało przewidziane już w komunikacie w sprawie europejskiego programu ochrony infrastruktury krytycznej, zaś CIWIN jako narzędzie informatyczne stanowi jeden z celów operacyjnych EPCIP. Niemniej jednak cel operacyjny (pośredni), jaki CIWIN zamierza osiągnąć, można określić w następujący sposób:

- zapewnienie narzędzia informatycznego ułatwiającego współpracę w zakresie ochrony infrastruktury krytycznej między państwami członkowskimi, które będzie stanowiło wydajną i szybką alternatywę dla często czasochłonnych metod poszukiwania informacji oraz które udostępni państwom członkowskim możliwość bezpośredniego kontaktowania się i zamieszczania informacji, które uważają za istotne.

5.4. Metoda realizacji (indykatywna)

☒ ***Zarządzanie scentralizowane***

☒ bezpośrednio przez Komisję

☐ pośrednio przez:

☐ agencje wykonawcze

☐ ustanowione przez Wspólnoty organy określone w art. 185 rozporządzenia finansowego

☐ krajowe organy sektora publicznego/organy pełniące misję służby publicznej

☐ ***Zarządzanie dzielone lub zdecentralizowane***

☐ z państwami członkowskimi

☐ z krajami trzecimi

☐ ***Zarządzanie wspólne z organizacjami międzynarodowymi (należy wyszczególnić)***

Uwagi:

6. MONITOROWANIE I OCENA

6.1. System monitorowania

Aby ocenić postępy CIWIN, należy zastosować następujące wskaźniki:

– liczba państw członkowskich uczestniczących w sieci CIWIN (przynajmniej 20 państw członkowskich powinno stosować system regularnie, aby można było uznać go za udany);

– poziom tajności wymienianych informacji (czy państwa członkowskie zamieszczają wyłącznie informacje nieoznaczone klauzulą tajności, czy również zamieszczane są informacje tajne);

– czy grupy specjalistów z zakresu ochrony infrastruktury krytycznej wykorzystują CIWIN jako główne narzędzie do wymiany opinii, aby osiągnąć swoje cele (np. definicja kryteriów określania infrastruktury krytycznej w poszczególnych sektorach)?

6.2. Ocena

6.2.1. Ocena ex-ante

Po zakończeniu okresu próbnego (projekt pilotażowy CIWIN) w 2009 r. Komisja wyśle krótkie ankiety do władz państw członkowskich, w których określą one poziom zadowolenia z pracy systemu oraz ocenią, czy system przyczynia się do zrealizowania ogólnych celów inicjatywy dotyczącej CIWIN (wraz z propozycjami wprowadzenia ewentualnych nowych funkcji lub usunięcia funkcji niedziałających dobrze).

Ponadto sporządzono ocenę skutków, która została załączona do niniejszego wniosku.

6.2.2. Działania podjęte w wyniku oceny pośredniej/ex-post (wnioski wyciągnięte z podobnych doświadczeń w przeszłości)

Główne rozwiązania w zakresie monitorowania i oceny powinny się opierać na zadowoleniu klienta.

– Raz na trzy lata Komisja powinna dokonywać oceny działającego systemu. Komisja powinna opierać swój przegląd na opiniach państw członkowskich uzyskanych podczas regularnych spotkań z udziałem przedstawicieli punktów kontaktowych ds. ochrony infrastruktury krytycznej.

6.2.3. Warunki i częstotliwość przyszłych ocen

Po trzech latach od utworzenia CIWIN należy poddać ocenie według wskaźników wymienionych w pkt 6.1.

7. ŚRODKI ZWALCZANIA NADUŻYĆ FINANSOWYCH

Ochrona interesów finansowych Wspólnoty oraz zwalczanie nadużyć finansowych i nieprawidłowości stanowią integralną część niniejszej decyzji.

Odpowiednie służby Komisji będą odpowiedzialne za administracyjne monitorowanie umów i płatności. Każda z operacji sfinansowanych na mocy niniejszej decyzji będzie nadzorowana

na wszystkich etapach cyklu projektu przez odpowiednie służby Komisji. Nadzór będzie uwzględniał zarówno obowiązki wynikające z umowy, jak i zasady analizy kosztów i korzyści oraz prawidłowego zarządzania finansami.

Ponadto jakiekolwiek porozumienie lub umowa zawarte zgodnie z niniejszą decyzją powinny wyraźnie przewidywać monitorowanie wydatków zaakceptowanych w ramach projektów/programów oraz właściwej realizacji działań, jak również kontrolę finansową prowadzoną przez Komisję, włączając Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz kontrole przeprowadzane przez Trybunał Obrachunkowy, w razie potrzeby na miejscu. Powinny również upoważniać Komisję (OLAF) do przeprowadzania kontroli na miejscu oraz inspekcji zgodnie z rozporządzeniem Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami.

Szczególną uwagę należy zwrócić na charakter wydatków (kwalifikowalność wydatków), przestrzegania budżetów (wydatki rzeczywiste) oraz sprawdzenie informacji uzupełniających oraz odpowiednich dokumentów (dowodów poniesienia wydatków).

8. SZCZEGÓŁOWE INFORMACJE DOTYCZĄCE ZASOBÓW

8.1. Cele wniosku z uwzględnieniem ich kosztu finansowego

Środki na zobowiązania w mln EUR (do 3 miejsc po przecinku)

(Należy wskazać cele, działania i realizacje)	**Rodzaj realizacji**	**Średni koszt**	2009 r.		**2010 r.**		**2011 r.**		**2012 r.**		**2013 r.**		**RAZEM**	
			Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity
CEL OPERACYJNY NR 1[10] **Zapewnienie narzędzia informatycznego, które ułatwi współpracę między państwami członkowskimi w zakresie ochrony infrastruktury krytycznej**														
Działanie: Stworzenie i zarządzanie systemem wczesnego ostrzegania w zakresie ochrony infrastruktury krytycznej oraz stworzenie forum														

[10] Zgodnie z opisem w sekcji 5.3.

(Należy wskazać cele, działania i realizacje)	Rodzaj realizacji	Średni koszt	2009 r.		2010 r.		2011 r.		2012 r.		2013 r.		RAZEM	
			Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity	Liczba realizacji	Koszt całkowity
wymiany najlepszych praktyk														
- Realizacja 1	Pełnienie funkcji systemu wczesnego ostrzegania przez system	0,3	1	0,3	1	0,3	1	0,3	1	0,3	1	0,3	5	1,5
- Realizacja 2	Wsparcie i utrzymanie systemu	0,25	1	0,25	1	0,25	1	0,25	1	0,25	1	0,25	5	1,25
- Realizacja 3	Niezbędne wsparcie techniczne dla akredytacji bezpieczeństwa, zarządzania, zapewnienia działów pomocy technicznej i szkoleń	0,07	1	0,4									1	0,4
KOSZT CAŁKOWITY 1		0, 617	1	0,95	1	0,55	1	0,55	1	0,55	1	0,55	5	3,15

8.2. Wydatki administracyjne

8.2.1. Liczba i rodzaj pracowników

Rodzaj stanowiska		Personel, któremu powierzono zarządzanie działaniem przy użyciu istniejących lub dodatkowych zasobów (**liczba stanowisk/pełnych etatów**)									
		2009 r.		2010 r.		2011 r.		2012 r.		2013 r.	
(18)	(20) AD	(21)	0,5	(22)	0,5	(23)	0,5	(24)	0,5	(25)	0,5
(19)	AST	0,5		0,5		0,5		0,5		0,5	
Urzędnicy i pracownicy zatrudnieni na czas określony[11] (XX 01 01)											
Pracownicy finansowani[12] w ramach art. XX 01 02											
Inni pracownicy[13] finansowani w ramach art. XX 01 04/05											
RAZEM		1		1		1		1		1	

8.2.2. Opis zadań związanych z działaniem

Głównym zadaniem urzędników Komisji będzie pełnienie funkcji administratora CIWIN. Urzędnicy Komisji będą zatem odpowiedzialni za konfigurację rozwiązań; będą zarządzać wnioskami o stworzenie obszarów dynamicznych oraz będą odpowiedzialni za ich tworzenie i usuwanie niewykorzystanych lub porzuconych obszarów. Rola administratora zostanie powierzona Komisji.

8.2.3. Źródła zasobów ludzkich (stosunek pracy)

☒ Stanowiska obecnie przypisane do zarządzania programem, które zostaną utrzymane lub przekształcone

[11] Koszty te NIE są uwzględnione w kwocie referencyjnej.
[12] Koszty te NIE są uwzględnione w kwocie referencyjnej.
[13] Koszty te są uwzględnione w kwocie referencyjnej.

- ☐ Stanowiska wstępnie przyznane w ramach rocznej strategii politycznej/wstępnego projektu budżetu (APS/PDB) na rok n

- ☐ Stanowiska, o które zostanie złożony wniosek w ramach następnej procedury APS/PDB

- ☐ Przesunięcia w ramach zasobów danej jednostki organizacyjnej (przesunięcia wewnętrzne)

- ☐ Stanowiska, których obsadzenie będzie konieczne w roku n, nieprzewidziane w APS/PDB na dany rok

8.2.4. Inne wydatki administracyjne uwzględnione w kwocie referencyjnej (XX 01 04/05 – wydatki na administrację i zarządzanie)

w mln EUR (do 3 miejsc po przecinku)

Pozycja w budżecie (numer i treść)	2009 r.	2010 r.	2011 r.	2012 r.	2013 r.	RAZEM
1 Pomoc techniczna i administracyjna (w tym powiązane koszty personelu)						
Agencje wykonawcze[14]	nd.	nd.	nd.	nd.	nd.	nd.
Inna pomoc techniczna i administracyjna	nd.	nd.	nd.	nd.	nd.	nd.
- wewnętrzna						
- zewnętrzna						
Pomoc techniczna i administracyjna ogółem	nd.	nd.	nd.	nd.	nd.	nd.

8.2.5. Koszt finansowy zasobów ludzkich i powiązane koszty nieuwzględnione w kwocie referencyjnej)

w mln EUR (do 3 miejsc po przecinku)

Rodzaj zasobów ludzkich	2009	2010	2011	2012	2013
Urzędnicy i pracownicy zatrudnieni na czas określony (XX 01 01)	0, 117	0, 117	0,117	0,117	0,117
Pracownicy finansowani w ramach art. XX 01 02 (personel pomocniczy, oddelegowani eksperci krajowi (END), personel kontraktowy itp.) (należy określić pozycję w budżecie)					
Koszt zasobów ludzkich i koszty powiązane (NIEUWZGLĘDNIONE w kwocie referencyjnej) ogółem	0,117	0,117	0,117	0,117	0,117

[14] Należy odnieść się do oceny skutków finansowych regulacji dla danej agencji wykonawczej/danych agencji wykonawczych.

Kalkulacja – ***urzędnicy i pracownicy zatrudnieni na czas określony***

Zob. pkt 8.2.1.

Kalkulacja – ***pracownicy finansowani w ramach art. XX 01 02***

nd.

	2009 r.	2010 r.	2011 r.	2012 r.	2013 r.	RAZEM
XX 01 02 11 01 — podróże służbowe	0,01	0,01	0,01	0,01	0,01	0,05
XX 01 02 11 02 — spotkania i konferencje	0,005	0,005	0,005	0,005	0,005	0,025
XX 01 02 11 03 — komitety[15]	nd.	nd.	nd.	nd.	nd.	nd.
XX 01 02 11 04 — badania i konsultacje	nd.	nd.	nd.	nd.	nd.	nd.
XX 01 02 11 05 — systemy informatyczne	nd.	nd.	nd.	nd.	nd.	nd.
2 Inne wydatki na zarządzanie ogółem (XX 01 02 11)	nd.	nd.	nd.	nd.	nd.	nd.
3 **Inne wydatki o charakterze administracyjnym** (należy wskazać jakie, odnosząc się do pozycji w budżecie)	nd.	nd.	nd.	nd.	nd.	nd.
Ogółem wydatki administracyjne inne niż wydatki na zasoby ludzkie i powiązane koszty (NIEUWZGLĘDNIONE w kwocie referencyjnej)	0,015	0,015	0,015	0,015	0,015	0,075

Kalkulacja – ***inne wydatki administracyjne <u>nieuwzględnione</u> w kwocie referencyjnej***

nd.

[15] Należy określić rodzaj komitetu i grupę, do której należy.