KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 20.10.2004
COM(2004) 702 końcowy

KOMUNIKAT KOMISJI
DO RADY I PARLAMENTU EUROPEJSKIEGO

Ochrona infrastruktury strategicznej w walce z terroryzmem

SPIS TREŚCI

1. WSTĘP 3

2. ZAGROŻENIE 3

3. EUROPEJSKA INFRASTRUKTURA STRATEGICZNA 3

3.1. Czym jest infrastruktura strategiczna 3

3.2. Zarządzanie bezpieczeństwem 5

4. DOTYCHCZASOWY POSTĘP W ZAKRESIE OCHRONY INFRASTRUKTURY STRATEGICZNEJ NA SZCZEBLU WSPÓLNOTOWYM 6

5. ZWIĘKSZANIE ZDOLNOŚCI OCHRONY INFRASTRUKTURY STRATEGICZNEJ UE 7

5.1. Europejski Program Ochrony Infrastruktury Strategicznej (EPOIS) 7

5.2. Wdrożenie EPOIS 9

5.3. Cele EPOIS i wskaźniki postępu 9

ZAŁĄCZNIK TECHNICZNY 11

1. WSTĘP

Rada Europejska na posiedzeniu w czerwcu 2004 r. zwróciła się do Komisji i Wysokiego Przedstawiciela o przygotowanie ogólnej strategii ochrony infrastruktury strategicznej.

Niniejszy komunikat stanowi zarys działań, jakie obecnie podejmuje Komisja w celu ochrony infrastruktury strategicznej oraz proponuje dodatkowe środki w celu wzmocnienia istniejących instrumentów i wypełnienia obowiązków powierzonych przez Radę Europejską.

2. ZAGROŻENIE

Rośnie prawdopodobieństwo katastrofalnych ataków terrorystycznych, których celem byłyby strategiczne zasoby infrastruktury. Konsekwencje ataku na systemy kontroli przemysłowej infrastruktury strategicznej mogą być bardzo różne. Powszechnie przyjmuje się, że udany atak informatyczny spowodowałby niewiele, jeśli w ogóle, ofiar w ludziach, ale jego efektem mogłaby być niemożność zapewnienia niezbędnych usług infrastrukturalnych. Na przykład, udany atak informatyczny na publiczną sieć łączności telefonicznej mógłby pozbawić użytkowników dostępu do usług telefonicznych do czasu, gdy technicy nie uruchomią i nie naprawią sieci. Atak na systemy kontroli zakładu chemicznego lub płynnego gazu ziemnego mógłby doprowadzić do śmierci większej liczby osób oraz do znacznych szkód fizycznych.

Innego rodzaju katastrofalna awaria mogłaby mieć miejsce, gdyby jedna część infrastruktury spowodowała uszkodzenie innych części, wywołując szeroko zakrojony efekt kaskadowy. Tego typu awaria mogłaby się wydarzyć na skutek efektu synergii pomiędzy poszczególnymi gałęziami przemysłu. Prostym przykładem jest atak na instalacje elektryczne, powodujący przerwę w dostawach energii elektrycznej; awarii mogą również ulec oczyszczalnie ścieków i sieć wodociągowa, ponieważ turbiny i inne urządzenia elektryczne w tych zakładach przestałyby działać.

Wydarzenia powstające kaskadowo mogą również wywołać wiele szkód, powodując zaburzenia w usługach na szeroką skalę. Przerwy w dostawie energii elektrycznej w Ameryce Północnej i Europie w ciągu ostatnich dwóch lat stanowią dowód na wrażliwość infrastruktur energetycznych i w związku z tym wskazują na potrzebę znalezienia skutecznych środków zapobiegania i/lub ograniczania konsekwencji poważnych przerw w dostawach energii. Konsekwencją takiego wykorzystania terroryzmu informatycznego mogłoby również być wzmocnienie skutków ataku fizycznego. Przykładem tego byłoby połączenie konwencjonalnego ataku bombowego na budynek z czasowym odłączeniem dostaw elektryczności lub usług telefonicznych. Wynikające z tego utrudnienie interwencji służb ratunkowych do czasu przywrócenia dostaw prądu lub możliwości komunikacyjnych mogłoby zwiększyć liczbę ofiar i panikę wśród ludzi.

3. EUROPEJSKA INFRASTRUKTURA STRATEGICZNA

3.1. Czym jest infrastruktura strategiczna

Infrastrukturą strategiczną są te zakłady fizyczne i urządzenia technologii informacyjnych, sieci, usługi i aktywa, których zakłócenie pracy lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrobyt ekonomiczny obywateli lub na skuteczność

funkcjonowania rządów w Państwach Członkowskich. Infrastruktura strategiczna obejmuje wiele sektorów gospodarki, w tym bankowość i finanse, transport i dystrybucję, energetykę, zakłady użyteczności publicznej, zdrowie, dostawy żywności i komunikację, jak również główne służby rządowe. Niektóre decydujące elementy w tych sektorach nie są „infrastrukturą" w ścisłym znaczeniu tego słowa, ale tak naprawdę sieciami lub łańcuchami dostaw wspierającymi dostarczanie zasadniczego produktu lub usługi. Na przykład, dostawa żywności lub wody do naszych największych obszarów miejskich zależy od pewnych kluczowych urządzeń użyteczności publicznej, ale także od złożonej sieci producentów, przetwórców, wytwórców, dystrybutorów i detalistów.

Infrastruktura strategiczna obejmuje:

- instalacje i sieci energetyczne (np. produkcja energii elektrycznej, ropy naftowej i gazu, magazyny i rafinerie, system transmisji i dystrybucji)

- technologie komunikacyjne i informacyjne (np. telekomunikacja, radio i telewizja, oprogramowanie, sprzęt i sieci komputerowe, w tym Internet)

- finanse (np. bankowość, papiery wartościowe i inwestycje)

- opiekę zdrowotną (np. szpitale, zakłady opieki zdrowotnej i punkty krwiodawstwa, laboratoria i farmaceutyki, poszukiwania i ratownictwo, pogotowie ratunkowe)

- żywność (np. bezpieczeństwo, środki produkcji, dystrybucja hurtowa i przemysł spożywczy).

- wodę (np. tamy, zbiorniki, oczyszczalnie i sieci wodociągowe)

- transport (np. lotniska, porty, urządzenia intermodalne, sieci kolejowe i tranzytu masowego, systemy kontroli ruchu)

- produkcję, składowanie i transport niebezpiecznych towarów (np. materiały chemiczne, biologiczne, radiologiczne i nuklearne)

- rząd (np. usługi podstawowe, urządzenia, sieci informacyjne, aktywa i kluczowe krajowe lokalizacje i pomniki).

Te elementy infrastruktury należą lub są eksploatowane zarówno przez sektor publiczny, jak i prywatny. Jednakże w komunikacie 574/2001 z dnia 10 października 2001 r. Komisja stwierdziła, że: „Wzmocnienie przez władze publiczne niektórych środków bezpieczeństwa w następstwie ataków skierowanych przeciwko społeczeństwu jako całości, a nie przeciwko przemysłowi, musi być ponoszone przez Państwo". Dlatego też sektor publiczny ma tu do odegrania zasadniczą rolę.

Elementy infrastruktury strategicznej muszą zostać określone na szczeblu Państw Członkowskich oraz na szczeblu europejskim, a wykazy takie powinny zostać opracowane do końca 2005 r.

Europejskie infrastruktury strategiczne są silnie powiązane i wzajemnie od siebie uzależnione. Konsolidacja spółek, racjonalizacja przemysłu, wydajne praktyki handlowe takie jak produkcja w systemie *just in time* oraz koncentracja populacji na obszarach miejskich,

przyczyniły się do tej sytuacji. Europejskie infrastruktury strategiczne stały się zależne w większym stopniu od wspólnych technologii informacyjnych obejmujących Internet oraz przestrzenną radionawigację i komunikację. W tych wzajemnie powiązanych infrastrukturach problemy mogą narastać kaskadowo, powodując nieoczekiwane i coraz poważniejsze awarie istotnych usług. Wzajemne powiązanie i współzależność infrastruktur sprawiają, że są one bardziej podatne na zakłócenia lub zniszczenie.

Należy zbadać kryteria dla ustalenia czynników decydujących o tym, że określona infrastruktura lub element infrastruktury ma znaczenie strategiczne. Takie kryteria selekcji powinny również zostać opracowane w oparciu o fachową wiedzę sektorową i zbiorową. Można zaproponować trzy czynniki dla identyfikacji potencjalnej infrastruktury strategicznej:

- Zakres – utratę elementu strategicznej infrastruktury ocenia się na podstawie wielkości obszaru geograficznego, który mógłby zostać dotknięty jego utratą lub niedostępnością – międzynarodowy, krajowy, prowincjalny/terytorialny lub lokalny.

- Waga – stopień wpływu lub utraty można ocenić jako: żaden, minimalny, umiarkowany lub poważny. Do kryteriów, które można wykorzystać do oceny potencjalnej wagi, należą:

    (a) wpływ społeczny (wielkość dotkniętej populacji, utrata życia, choroba, poważne uszkodzenie ciała, ewakuacja);

    (b) wpływ gospodarczy (oddziaływanie na PKB, znaczenie strat gospodarczych i/lub pogorszenie produktów lub usług);

    (c) wpływ ekologiczny (wpływ na społeczeństwo i środowisko); oraz

    (d) współzależność (z innymi elementami infrastruktury strategicznej);

    (e) wpływ polityczny (zaufanie w umiejętności rządu);

- Skutki czasowe – to kryterium określa, w jakim momencie utrata elementu mogłaby mieć poważny wpływ (tj. natychmiast, w 24-48 godzin, za tydzień, inny).

Jednakże w wielu wypadkach efekty psychologiczne mogą spotęgować wagę wydarzenia o niewielkim poza tym znaczeniu.

Bieżący rozwój ochrony infrastruktury strategicznej udokumentowano w załączniku technicznym, który przedstawia sektorowy bilans dotychczasowych osiągnięć Komisji. Pokazują one, że Komisja zdobyła w tej dziedzinie znaczne doświadczenie.

3.2. Zarządzanie bezpieczeństwem

Do przeprowadzenia analizy zagrożeń, wypadków i podatności elementów infrastruktury strategicznej Państw Członkowskich i ich zależności, potrzebne są informacje pochodzące z pewnej liczby źródeł. Każdy sektor i każde Państwo Członkowskie będzie musiało ustalić, jaka infrastruktura ma dla niego znaczenie strategiczne w obrębie ich odpowiednich jurysdykcji, zgodnie ze zharmonizowanym wzorem UE, oraz organizacje lub osoby odpowiedzialne za bezpieczeństwo.

Nie wszystkie rodzaje infrastruktury można ochronić przed wszelkimi zagrożeniami. Na przykład, elektryczne sieci transmisyjne są zbyt duże, żeby je ogrodzić lub pilnować. Stosując

techniki zarządzania ryzykiem można skupić uwagę na obszarach największego ryzyka uwzględniając zagrożenie, względny strategiczny charakter, istniejący poziom ochrony oraz skuteczność dostępnych strategii ograniczania wypadków dla zapewnienia ciągłości działań.

Zarządzanie bezpieczeństwem to zamierzony proces rozumienia ryzyka i podejmowania decyzji oraz wdrażania działań mających na celu ograniczenie ryzyka do określonego poziomu, który jest akceptowalnym poziomem ryzyka przy akceptowalnym koszcie. Takie podejście charakteryzuje się identyfikowaniem, pomiarem i kontrolą ryzyk współmiernie do wyznaczonego poziomu.

Ochrona infrastruktury strategicznej (OIS) wymaga konsekwentnego, opartego na współpracy partnerstwa między właścicielami i operatorami infrastruktury strategicznej a władzami Państw Członkowskich. Odpowiedzialność za zarządzanie ryzykiem w fizycznych zakładach, łańcuchach dostaw, technologiach informacyjnych i sieciach komunikacyjnych spoczywa przede wszystkim na właścicielach i operatorach.

Należy ogłaszać alerty, powiadomienia i noty informacyjne, aby pomóc uczestnikom z sektora publicznego i prywatnego chronić kluczowe systemy infrastrukturalne. Od czasu do czasu mogą się pojawić określone ryzyka lub zagrożenia atakiem terrorystycznym wymagające natychmiastowej reakcji. W takich sytuacjach od rządów i przemysłu Państw Członkowskich wymagana będzie dobrze skoordynowana i operacyjnie skoncentrowana reakcja, a UE powinna koordynować konieczne reakcje polityczne, na której to podstawie zawierane będą z zainteresowanymi stronami dodatkowe szczegółowe porozumienia w poszczególnych przypadkach.

Nawet najlepsze plany zarządzania bezpieczeństwem i ustawodawstwo zobowiązujące do ich stosowania są bezwartościowe, jeżeli brak jest ich prawidłowego wdrożenia. Doświadczenie pokazuje, że niezależne kontrole bezpieczeństwa przeprowadzane przez Komisję dotyczące wdrożenia przepisów stanowią jedyny skuteczny instrument gwarantujący prawidłowe wdrożenie wymogów bezpieczeństwa.

4. DOTYCHCZASOWY POSTĘP W ZAKRESIE OCHRONY INFRASTRUKTURY STRATEGICZNEJ NA SZCZEBLU WSPÓLNOTOWYM

Europejczycy oczekują, że infrastruktura strategiczna będzie funkcjonować bez względu na to, jakie organizacje są właścicielami lub eksploatują jej części składowe. Oczekują oni, że rządy Państw Członkowskich i UE będą odgrywać wiodącą rolę w zagwarantowaniu ich działania. Spodziewają się, że władze na wszystkich szczeblach oraz właściciele i operatorzy sektora prywatnego będą współpracować w celu zapewnienia ciągłości dostaw usług, od których Europejczycy są zależni.

W ramach uzupełnienia środków wprowadzonych na szczeblu krajowym Unia Europejska podjęła już kilka inicjatyw ustawodawczych ustanawiających minimalne standardy ochrony infrastruktury w ramach różnych polityk unijnych. Odnosi się to zwłaszcza do sektorów transportu, komunikacji, energetyki, BHP oraz sektora zdrowia publicznego. Działania zintensyfikowano po ostatnich zamachach w Ameryce i w Europie. Doprowadzą one do dalszego ulepszenia lub rozszerzenia istniejących środków.

Przez dziesięciolecia w ramach Traktatu EURATOM prowadzono inspekcje w celu kontrolowania prawidłowego wykorzystania materiałów nuklearnych. Na polu ochrony przed

promieniowaniem istnieje znaczna liczba aktów prawnych dotyczących zagrożeń związanych z działalnością zakładów i korzystaniem ze źródeł obejmujących substancje radioaktywne.

W dziedzinie transportu międzynarodowego Unia Europejska przyjęła ustawodawstwo wdrażające lub wzmacniające porozumienia zawarte przez międzynarodowe organy zarządzające w sektorze lotniczym i transporcie morskim. Unia Europejska będzie nadal promować i aktywnie uczestniczyć w ich działaniach na szczeblu międzynarodowym. Będzie ona zachęcać państwa trzecie powiązane gospodarczo z UE do wdrażania tych porozumień. W odniesieniu do niektórych z nich udzieliła pewnego wsparcia w celu osiągnięcia jednolitego i stałego poziomu bezpieczeństwa w obrębie i poza granicami UE.

Kolejnym krokiem jest utworzenie agencji takich, jak Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) dla zapewnienia bezpieczeństwa komunikacji. Ponadto, w dziedzinach takich jak bezpieczeństwo lotnicze i morskie w ramach Komisji utworzono służby kontrolne mające na celu kontrolę wdrażania przez Państwa Członkowskie ustawodawstwa dotyczącego bezpieczeństwa. Kontrole te tworzą niezbędny punkt odniesienia gwarantujący jednakowy poziom wdrażania w całej Unii.

Bieżący rozwój w dziedzinie ochrony infrastruktury strategicznej udokumentowano w załączniku technicznym, który przedstawia sektorowy bilans dotychczasowych osiągnięć Komisji. Pokazują one, że Komisja zdobyła w tej dziedzinie znaczne doświadczenie.

5. ZWIĘKSZANIE ZDOLNOŚCI OCHRONY INFRASTRUKTURY STRATEGICZNEJ UE

5.1. Europejski Program Ochrony Infrastruktury Strategicznej (EPOIS)

Z uwagi na dużą ilość potencjalnie strategicznych infrastruktur i ich specyfikę, niemożliwa jest ochrona ich wszystkich przey użyciu środków oddziaływujących na szczeblu europejskim. Stosując zasadę pomocniczości Europa musi koncentrować swoje wysiłki na ochronie infrastruktur o znaczeniu ponadgranicznym i poddać inne pod wyłączną odpowiedzialność Państw Członkowskich, ale podlegające pod wspólne ramy.

Istnieją już liczne dyrektywy i rozporządzenia wprowadzające środki mające na celu wykrywanie wypadków, określanie planów interwencji we współpracy z Obroną Cywilną, regularne ćwiczenia i wyraźne powiązania między różnymi poziomami interwencji, władzą publiczną, organizacjami centralnymi i służbami ratowniczymi. Z drugiej strony pozostaje jeszcze wiele do zrobienia w zakresie ochrony instalacji energetycznych, innych niż atomowe. Jak wskazano w załączniku technicznym, acquis communautaire w zakresie ochrony strategicznych infrastruktur istnieje w różnych stadiach zaawansowania.

W większości dziedzin wymienionych wyżej prace trwają oraz nawiązano współpracę z ekspertami z Państw Członkowskich i zainteresowanymi gałęziami gospodarki w celu identyfikacji potencjalnych niedociągnięć i środków naprawczych, które należy zastosować (prawnych lub innych). Utworzono wiele sieci i komitetów bezpieczeństwa.

Komisja, w drodze komunikatu, będzie zdawać innym instytucjom coroczne sprawozdania z dokonanego postępu. Przeanalizuje ona dla każdego sektora ewolucję w pracach Wspólnoty na polu oceny ryzyka, rozwoju technik ochrony lub trwających/przewidywanych działań prawnych w celu zebrania opinii. Ponadto, Komisja w razie potrzeby zaproponuje w tym

komunikacie aktualizacje i poziome środki organizacyjne, w wypadku których istnieje potrzeba ujednolicenia, koordynacji lub współpracy. Komunikat ten, zawierający wszelkie analizy sektorowe i środki, będzie stanowił podstawę dla Europejskiego Programu Ochrony Infrastruktury Strategicznej (EPOIS).

Program ten będzie dążył do wspierania przemysłu i rządów Państw Członkowskich na wszystkich szczeblach w UE uwzględniając jednocześnie indywidualne uprawnienia i odpowiedzialności. Komisja jest zdania, że sieć skupiająca specjalistów do spraw OIS z Państw Członkowskich UE może wspierać Komisję w przygotowaniu programu – ta Ostrzegawcza Sieć Informacyjna dla Infrastruktury Strategicznej (OSIIS) powinna zostać utworzona jak najszybciej w 2005 r.

Stworzenie sieci powinno przede wszystkim pomóc w stymulowaniu wymiany informacji na temat wspólnych zagrożeń i słabości oraz odpowiednich środków i strategii ograniczania ryzyka dla wspierania ochrony infrastruktury strategicznej. Państwa Członkowskie z ich strony powinny upewnić się, że istotne informacje są przekazywane wszystkim odpowiednim departamentom i agencjom rządowym, w tym organizacjom zajmującym się ratownictwem, przekazując dane odpowiednim organom z sektorów przemysłu, które z kolei będą informować danych właścicieli i operatorów infrastruktury strategicznej za pośrednictwem sieci kontaktów utworzonej w Państwach Członkowskich.

EPOIS promowałaby stałe forum, na którym ograniczenia powodowane przez konkurencję, odpowiedzialność i wrażliwość na informacje możnaby zrównoważyć korzyściami płynącymi z bezpieczniejszej infrastruktury strategicznej. W procesie tym przemysł będzie szczegółowo konsultowany. Pomoże to dostarczyć partnerom większą liczbę informacji na temat określonych sytuacji zagrożenia, co pozwoli im na podjęcie działań w celu zaradzenia potencjalnym konsekwencjom. Odpowiedzialność właścicieli i operatorów za podejmowanie ich własnych decyzji i tworzenia planów ochrony dotyczących należącego do nich majątku nie powinna ulec zmianie.

Tam, gdzie brak jest norm sektorowych lub gdzie nie zostały jeszcze stworzone międzynarodowe normy, Europejski Komitet Normalizacyjny (CEN) i inne odpowiednie organizacje normalizacyjne mogłyby wspierać sieć i proponować jednolite sektorowe i przystosowane normy bezpieczeństwa dla wszystkich zainteresowanych gałęzi i sektorów. Takie normy powinno się również zaproponować na szczeblu międzynarodowym poprzez ISO, aby ustalić w tym zakresie właściwe zasady działania.

Należy zachować ostrożność odnosząc się do krajowych zagrożeń dotyczących bezpieczeństwa infrastruktury strategicznej, w tym zagrożenia terroryzmem, aby uniknąć niepotrzebnego niepokoju wewnętrznego w UE oraz ze strony potencjalnych turystów i inwestorów. Terroryzm stanowi stałe zagrożenie, ale zadaniem polityków jest zachęcania wszystkich do tego, aby nadal prowadzili życie w możliwie normalny sposób. Należy również zachować ostrożność, aby zagwarantować poszanowanie prawa prywatności, zarówno wewnątrz, jak i poza Unią. Konsumenci i operatorzy muszą być przekonani, że informacje będą przetwarzane właściwie, w sposób poufny i wiarygodny. Niezbędne jest utworzenie odpowiednich ram w celu zagwarantowania prawidłowego zarządzania zastrzeżonymi informacjami i ich ochrony przed wykorzystaniem przez nieupoważnione osoby lub ujawnieniem.

Duża część infrastruktury strategicznej UE oraz Państw Członkowskich wykracza poza granice UE. Rurociągi przebiegają w poprzek całych kontynentów, okablowanie o

kluczowym znaczeniu dla usług informacyjnych ukryte jest głęboko pod dnem oceanu itp. Oznacza to, że współpraca międzynarodowa stanowi ważny składnik tworzenia stałego, dynamicznego krajowego i międzynarodowego partnerstwa pomiędzy właścicielami/operatorami infrastruktury strategicznej i rządami państw trzecich, a zwłaszcza bezpośrednimi dostawcami produktów energetycznych do Unii.

5.2. Wdrożenie EPOIS

Ochrona infrastruktury strategicznej (OIS) wymaga aktywnego uczestnictwa jej właścicieli i operatorów, instytucji nadzorujących, organów zawodowych, stowarzyszeń przemysłowych, Państw Członkowskich oraz Komisji. Zadaniem EPOIS realizowanym w oparciu o informacje dostarczone przez interfejsy i sieć Państw Członkowskich będzie dalsze identyfikowanie infrastruktury strategicznej, analiza wrażliwości i współzależności oraz wychodzenie z rozwiązaniami mającymi na celu ochronę przed i przygotowanie się na wszelkie zagrożenia. Objęłaby ona wsparcie dla sektorów przemysłu w zrozumieniu zagrożeń i skutków w ich ocenach ryzyka. Organy zajmujące się egzekwowaniem prawa w Państwach Członkowskich oraz mechanizm ochrony cywilnej powinny zagwarantować, że EPOIS stanie się integralną częścią ich procesu planowania i podnoszenia świadomości.

Służby Komisji, w ścisłej koordynacji z siecią, rozwiną dalsze działania, które powinny polegać na przyjmowaniu ustawodawstwa i/lub rozpowszechnianiu informacji. Oddziały specjalne policji i Europolu miałyby do odegrania rolę w rozpowszechnianiu istotnych informacji o poziomach bezpieczeństwa i informacji wywiadowczych skierowanych do organów zajmujących się egzekwowaniem prawa w Państwach Członkowskich, a te z kolei powinny doradzać i współpracować z właścicielami i operatorami infrastruktury strategicznej w zakresie istotnego informowania o zagrożeniach, wsparcia w zapewnieniu doradztwa na temat ochrony i bezpieczeństwa oraz rozwoju strategii ochrony w celu przeciwdziałania terroryzmowi.

Rządy Państw Członkowskich będą kontynuować i/lub rozwijać i utrzymywać bazy danych infrastruktury strategicznej o znaczeniu krajowym oraz będą odpowiedzialne za rozwój, uprawomocnianie i kontrolę istotnych planów w celu zapewnienia ciągłości usług w ramach swojej jurysdykcji. Przy opracowaniu EPOIS Komisja wysunie sugestie, co do tego, jaka powinna być minimalna zawartość i format takich baz danych i w jaki sposób powinny one być wzajemnie powiązane.

Z kolei rządy Państw Członkowskich będą nadal przekazywać właścicielom i operatorom infrastruktury strategicznej (oraz w razie potrzeby innym Państwom Członkowskim) istotne informacje wywiadowcze i alerty oraz, zainteresowanym stronom, uzgodnione oczekiwane odpowiedzi na każdy poziom zagrożenia/alertu.

Właściciele i operatorzy infrastruktury strategicznej zapewnią odpowiednie bezpieczeństwo ich majątku przez aktywne wdrażanie planów bezpieczeństwa oraz regularne inspekcje, ćwiczenia, oceny i plany. Państwa Członkowskie powinny kontrolować ogólny proces, podczas gdy Komisja powinna zapewnić jednakową procedurę wdrażania w całej Unii przy pomocy odpowiednich systemów kontroli.

5.3. Cele EPOIS i wskaźniki postępu

Celem EPOIS i obowiązkiem Komisji byłoby zapewnienie istnienia odpowiednich i jednakowych poziomów ochrony infrastruktury strategicznej, ograniczenie awarii do

minimum oraz dostarczenie szybkich i sprawdzonych środków naprawczych w całej Unii. EPOIS byłby stałym procesem i konieczne będzie dokonywanie jego regularnych przeglądów w zależności od rozwoju wydarzeń i obaw we Wspólnocie.

Sukces będzie mierzony w oparciu o:

- identyfikację i utworzenie przez rządy Państw Członkowskich spisów zasobów infrastruktury strategicznej podlegających ich jurysdykcji, zgodnie z priorytetami EPOIS;

- firmy współpracujące w ramach sektorów i współpracujące z rządem w celu wymiany informacji i zmniejszenia prawdopodobieństwa wystąpienia wypadków powodujących szeroko zakrojone lub długotrwałe przerwy w działaniu infrastruktur strategicznych;

- Wspólnota Europejska postanawia opracować wspólne podejście w kwestii ochrony infrastruktur strategicznych przez współpracę wszystkich aktorów sektora publicznego i prywatnego.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

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

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.