KOMISJA EUROPEJSKA

Bruksela, dnia 22.11.2010
KOM(2010) 673 wersja ostateczna

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy

1. EUROPEJSKI MODEL BEZPIECZEŃSTWA: WSPÓLNA PRACA NA RZECZ BEZPIECZNIEJSZEJ EUROPY

Większość Europejczyków może zajmować się życiem codziennym, nie musząc się martwić o swoje bezpieczeństwo. Nasze społeczeństwa są jednak narażone na poważne zagrożenia bezpieczeństwa, których skala i stopień skomplikowania stale wzrastają. Wiele z dzisiejszych zagrożeń dla bezpieczeństwa ma charakter transgraniczny i ponadsektorowy. Żadne państwo członkowskie nie jest w stanie poradzić sobie z nimi samo. Niepokoi to naszych obywateli i nasze przedsiębiorstwa. Czterech na pięciu Europejczyków chce, by na szczeblu UE podejmowano więcej działań przeciwko zorganizowanej przestępczości i terroryzmowi[1].

Wiele już osiągnięto, by przeciwdziałać tym pojawiającym się zagrożeniom i zwiększyć bezpieczeństwo Europy. Po wejściu w życie traktatu lizbońskiego[2] UE ma teraz możliwość – na podstawie wytycznych określonych w programie sztokholmskim i związanym z nim planie działania[3] – podjęcia dalszych zdecydowanych kroków. W strategii bezpieczeństwa wewnętrznego, która została przyjęta na początku 2010 r. podczas prezydencji hiszpańskiej[4], określono wyzwania, zasady i wytyczne dotyczące podejścia do tych kwestii w UE oraz wezwano Komisję do zaproponowania działań mających na celu wdrożenie tej strategii. Niniejszy komunikat – Strategia bezpieczeństwa wewnętrznego UE w działaniu – opiera się zatem na kwestiach uzgodnionych już przez państwa członkowskie i instytucje UE. Zawiera ona propozycje wspólnych działań, przy pomocy których przez następne cztery lata będziemy mogli bardziej skutecznie zwalczać **poważne przestępstwa, przestępczość zorganizowaną, terroryzm** i **cyberprzestępczość** oraz zapobiegać tym zjawiskom, jak również lepiej kontrolować **nasze granice zewnętrzne** i zwiększać **odporność na klęski żywiołowe i katastrofy spowodowane przez człowieka**.

Wspólny plan w obliczu wspólnych wyzwań

Rola UE w kwestii naszego bezpieczeństwa wewnętrznego polega na opracowywaniu wspólnych strategii politycznych i przepisów prawnych oraz wspieraniu praktycznej współpracy w takich dziedzinach jak współpraca policyjna i sądowa, zarządzanie granicami i zarządzanie kryzysowe. W drodze do osiągnięcia naszych celów bezpieczeństwa kluczowe znaczenie ma wkład zarówno polityki wewnętrznej, jak i zewnętrznej UE.

---

1 Eurobarometr 71, badanie standardowe.

2 Traktat o funkcjonowaniu Unii Europejskiej (TFUE).

3 Program sztokholmski – Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli (dokument Rady 17024/09); Przestrzeń wolności, bezpieczeństwa i sprawiedliwości: Plan działań służący realizacji programu sztokholmskiego – COM (2010) 171. Program sztokholmski jest programem UE w dziedzinie sprawiedliwości i spraw wewnętrznych na lata 2010–2014.

4 Dokument Rady, 5842/2/10, Projekt strategii bezpieczeństwa wewnętrznego Unii Europejskiej: Dążąc do europejskiego modelu bezpieczeństwa.

Dlatego też strategia bezpieczeństwa wewnętrznego UE przewiduje opracowanie wspólnego programu dla państw członkowskich, Parlamentu Europejskiego, Komisji, Rady, agencji i innych podmiotów, włączając w to społeczeństwo obywatelskie i władze lokalne. Program ten powinien być wspierany przez silny sektor bezpieczeństwa w UE, w którym producenci i usługodawcy ściśle współpracują z użytkownikami końcowymi. Nasze wspólne starania w celu znalezienia odpowiedzi na dzisiejsze wyzwania dla bezpieczeństwa wniosą również wkład w ugruntowanie i dalszy rozwój europejskiego modelu społecznej gospodarki rynkowej, który został przedstawiony w strategii „Europa 2020".

Polityka bezpieczeństwa oparta na wspólnych wartościach

Strategia bezpieczeństwa wewnętrznego UE oraz instrumenty i działania na rzecz jej realizacji muszą opierać się na wspólnych wartościach, do których należą praworządność i poszanowanie praw podstawowych, jak to zostało określone w **Karcie praw podstawowych Unii Europejskiej**[5]. Nasza koncepcja zarządzania kryzysowego musi charakteryzować się solidarnością. Polityka dotycząca zwalczania terroryzmu powinna być proporcjonalna do skali zagrożenia i mieć przede wszystkim na celu zapobieganie atakom w przyszłości. W przypadkach, gdy ma miejsce wymiana informacji służąca egzekwowaniu prawa w UE, musimy zadbać także o ochronę sfery prywatnej osób i ich podstawowego prawa do ochrony danych osobowych.

Bezpieczeństwo wewnętrzne w kontekście światowym

Bezpieczeństwa wewnętrznego nie można zagwarantować w odizolowaniu od reszty świata. W związku z tym ważne jest zapewnienie spójności i komplementarności pomiędzy wewnętrznymi i zewnętrznymi aspektami bezpieczeństwa UE. Wartości i priorytety, na których opiera się strategia bezpieczeństwa wewnętrznego, w tym nasze zaangażowanie na rzecz praw człowieka, demokracji, pokoju i stabilności w naszym sąsiedztwie oraz poza nim, są integralną częścią składową podejścia określonego w europejskiej strategii bezpieczeństwa[6]. Zgodnie z tą strategią zasadnicze znaczenie w walce przeciwko poważnym przestępstwom, przestępczości zorganizowanej i terroryzmowi mają stosunki z naszymi partnerami, w szczególności ze Stanami Zjednoczonymi.

Bezpieczeństwo powinno być nieodłącznym elementem właściwych strategicznych partnerstw. Należy je również wziąć pod uwagę w dialogu z naszymi partnerami w trakcie określania finansowania UE w umowach o partnerstwie. Zwłaszcza priorytety związane z bezpieczeństwem wewnętrznym powinny być wyraźnie podkreślane w dialogu politycznym z państwami trzecimi i organizacjami regionalnymi, tam gdzie jest to stosowne i istotne dla zwalczania licznych wektorów zagrożeń, takich jak handel ludźmi, handel narkotykami i terroryzm. Unia Europejska będzie oprócz tego zwracać szczególną uwagę na państwa trzecie i regiony, które nie tylko z punktu widzenia bezpieczeństwa zewnętrznego, lecz również bezpieczeństwa wewnętrznego mogą potrzebować wsparcia i wiedzy fachowej ze strony UE i państw członkowskich. Europejska Służba Działań Zewnętrznych umożliwi zintegrowanie dalszych działań i wiedzy fachowej poprzez wykorzystanie zdolności i know-how państw

---

5 „Strategia skutecznego wprowadzania w życie Karty praw podstawowych przez Unię Europejską" – COM (2010) 573.

6 „Europejska strategia bezpieczeństwa: Bezpieczna Europa w lepszym świecie" została przyjęta w 2003 r., zaś jej przeglądu dokonano w 2008 r.

członkowskich, Rady i Komisji. Do delegatur UE, w szczególności tych znajdujących się w państwach priorytetowych, należy przekazywać wiedzę ekspercką z zakresu bezpieczeństwa. Obejmuje to oddelegowywanie oficerów łącznikowych Europolu i sędziów łącznikowych[7]. Odpowiednie obowiązki i funkcje tych ekspertów zostaną określone przez Komisję i Europejską Służbę Działań Zewnętrznych.

2. PIĘĆ STRATEGICZNYCH CELÓW BEZPIECZEŃSTWA WEWNĘTRZNEGO

W niniejszym komunikacie przedstawiono najpilniejsze wyzwania dla bezpieczeństwa UE w nadchodzących latach. Zaproponowano pięć celów strategicznych i konkretne działania na lata 2011–2014, które wraz z dotychczasowymi staraniami i inicjatywami pomogą podnieść bezpieczeństwo w UE.

Poważne przestępstwa i przestępczość zorganizowana przyjmują rozmaite formy: handel ludźmi, handel narkotykami i bronią palną, pranie pieniędzy oraz nielegalne przewożenie i usuwanie odpadów w Europie i poza nią. Nawet na pozór drobne przestępstwa, takie jak włamania i kradzieże samochodów, handel towarami podrabianymi i niebezpiecznymi oraz działania gangów wędrownych, są często lokalnymi przejawami działalności światowych siatek przestępczych. Na przestępstwa te należy reagować wspólnym działaniem europejskim. Podobnie jest z **terroryzmem**: nasze społeczeństwa mogą być nadal celami ataków, takich jak zamachy bombowe w 2004 r. w Madrycie i w 2005 r. w Londynie. Musimy zatem działać ze zdwojoną siłą i ściślej współpracować, by zapobiec nowym zamachom.

Innym wzrastającym zagrożeniem jest **cyberprzestępczość**. Europa jest głównym celem cyberprzestępczości ze względu na swoją zaawansowaną infrastrukturę internetową, dużą ilość użytkowników, internetowy handel i internetowe systemy płatnicze. Należy wzmocnić ochronę obywateli, przedsiębiorstw i infrastruktury krytycznej przed przestępcami, którzy korzystają z nowoczesnych technologii. Również **bezpieczeństwo granic** wymaga bardziej spójnego działania. Ze względu na istnienie wspólnych granic zewnętrznych przemyt i inne rodzaje nielegalnej działalności transgranicznej należy zwalczać na szczeblu europejskim. Dlatego też istotnym elementem przestrzeni swobodnego przepływu jest skuteczna kontrola granic zewnętrznych UE.

Ponadto w ostatnich latach w Europie i jej bezpośrednim sąsiedztwie mamy do czynienia ze zwiększeniem częstotliwości i skali **klęsk żywiołowych i katastrof** spowodowanych przez człowieka. Ukazuje to potrzebę lepszej, bardziej spójnej i lepiej zintegrowanej zdolności Unii do reagowania na sytuacje kryzysowe i klęski żywiołowe, jak również wdrażania istniejących koncepcji i przepisów dotyczących zapobiegania skutkom katastrof.

CEL 1: Rozbijanie międzynarodowych siatek przestępczych

Mimo coraz bardziej intensywnej współpracy między organami ścigania i sądownictwem wewnątrz poszczególnych państw członkowskich oraz między nimi międzynarodowe siatki przestępcze pozostają niezwykle aktywne i czerpią ogromne zyski z działalności przestępczej. Oprócz korupcji i zastraszania miejscowej ludności oraz władz środki te są wykorzystywane często do infiltracji gospodarki i podkopywania zaufania publicznego.

---

[7] Zgodnie z decyzją Rady w sprawie Eurojustu 2009/426/WSiSW, którą należy transponować do czerwca 2011 r.

By zapobiegać przestępczości, konieczne jest zatem rozbijanie siatek przestępczych i zwalczanie bodźców finansowych, którymi się one kierują. W tym celu należy wzmocnić praktyczną współpracę organów ścigania. Organy ze wszystkich sektorów i na różnych płaszczyznach powinny współpracować ze sobą w celu ochrony gospodarki, a zyski pochodzące z działalności przestępczej powinny być skutecznie wykrywane i konfiskowane. Oprócz tego musimy także pokonać przeszkody, które wynikają z różnego podejścia stosowanego przez poszczególne państwa członkowskie, w razie potrzeby poprzez przepisy dotyczące współpracy sądowej, by ugruntować wzajemne uznawanie oraz wspólne definicje przestępstw kryminalnych i minimalny wymiar sankcji karnych[8].

Działanie 1: Wykrywanie i rozbijanie siatek przestępczych

W celu wykrywania i rozbijania siatek przestępczych istotna jest wiedza na temat metod działania ich członków oraz ich środków finansowych.

Komisja przedstawi zatem w 2011 r. wniosek legislacyjny w sprawie gromadzenia **danych dotyczących przelotu pasażerów** przekraczających zewnętrzną granicę UE drogą lotniczą. Organy w państwach członkowskich będą analizować te dane, co pomoże im w zapobieganiu atakom terrorystycznym i poważnym przestępstwom oraz w ich ściganiu.

Aby móc określić, czy środki finansowe pochodzą z działalności przestępczej i dokąd trafiają, konieczne są informacje na temat właścicieli spółek oraz funduszy powierniczych, przez które środki te przepływają. W praktyce organy ścigania i sądy, administracyjne organy dochodzeniowo-śledcze, takie jak OLAF, oraz fachowcy pochodzący z sektora prywatnego mają trudności z uzyskaniem takich informacji. Dlatego też – w kontekście dyskusji z międzynarodowymi partnerami w ramach Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy – UE powinna rozważyć dokonanie do 2013 r. przeglądu **unijnych przepisów dotyczących przeciwdziałania praniu pieniędzy**, by zwiększyć przejrzystość osób prawnych i uregulowań prawnych. Niektóre państwa członkowskie utworzyły centralny rejestr rachunków bankowych, by móc śledzić przepływy środków pochodzących ze źródeł przestępczych. Komisja opracuje w 2012 r. nowe wytyczne, aby zmaksymalizować przydatność takich rejestrów do egzekwowania prawa. By móc skutecznie prowadzić dochodzenia w sprawie przestępczych transakcji finansowych, organy ścigania i sądy powinny być wyposażone w niezbędne środki do gromadzenia, analizy i ewentualnego przekazywania informacji oraz powinny być przeszkolone w tym zakresie. Należy wykorzystać do tego celu programy szkoleniowe krajowych centrów doskonałości w dziedzinie śledztw finansowych oraz Europejskiego Kolegium Policyjnego (CEPOL). Komisja przedstawi w 2012 r. strategię w tej dziedzinie.

Ze względu na międzynarodowy charakter siatek przestępczych konieczne jest także nasilenie **wspólnych operacji** policji, służb celnych, straży granicznej i organów sądownictwa z poszczególnych państw członkowskich współpracujących z Eurojustem, Europolem i OLAF-em. Tego rodzaju operacje, obejmujące również tworzenie **wspólnych zespołów**

[8] Niedawne wnioski dotyczące dyrektywy w sprawie handlu ludźmi, seksualnego wykorzystywania dzieci i cyberprzestępczości stanowią ważny pierwszy krok w tym kierunku. W art. 83 ust. 1 TFUE wyszczególniono także inne dziedziny poważnej przestępczości: terroryzm, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, fałszowanie środków płatniczych i przestępczość zorganizowana.

dochodzeniowo-śledczych[9], powinny być przeprowadzane – jeśli to konieczne również w trybie pilnym – przy pełnym wsparciu ze strony Komisji zgodnie z priorytetami, strategicznymi celami i planami określonymi przez Radę na podstawie odpowiedniej analizy zagrożeń[10].

Ponadto Komisja i państwa członkowskie powinny w dalszym ciągu zapewniać skuteczność wdrażania **europejskiego nakazu aresztowania** oraz przedkładać informacje na temat jego stosowania, w tym jego skutków dla praw podstawowych.

Działanie 2: Ochrona gospodarki przed infiltracją przestępczą

Siatki przestępcze posługują się korupcją, by móc inwestować swoje zyski w legalnym obrocie gospodarczym, podkopując w ten sposób zaufanie do instytucji publicznych i systemu gospodarczego. Niewzruszona wola polityczna do walki z korupcją ma tu istotne znaczenie. Dlatego też niezbędne są działania na płaszczyźnie UE oraz wymiana najlepszych praktyk. W 2011 r. Komisja przedłoży wniosek dotyczący wsparcia dla **antykorupcyjnych działań państw członkowskich** oraz ich monitorowania.

W celu ochrony gospodarki przed infiltracją ze strony siatek przestępczych należy opracować strategie włączające do działania organy rządowe i regulacyjne właściwe do spraw udzielania licencji, zezwoleń, zamówień publicznych i dotacji (**podejście administracyjne**). Praktycznym wsparciem dla państw członkowskich ze strony Komisji będzie utworzenie przez nią w 2011 r. sieci krajowych punktów kontaktowych, które będą miały za zadanie wspierać wymianę najlepszych praktyk, oraz finansowanie przez Komisję projektów pilotażowych w konkretnych kwestiach praktycznych.

Towary podrobione przynoszą zorganizowanym grupom przestępczym duże zyski, wypaczają wzorce handlowe jednolitego rynku, mają szkodliwy wpływ na europejski przemysł i narażają na ryzyko zdrowie i bezpieczeństwo europejskich obywateli. Dlatego też w kontekście planu działania przeciwko podrabianiu i piractwie, który zostanie wkrótce przyjęty, Komisja podejmie wszelkie stosowne kroki w celu poprawy **egzekwowania praw własności intelektualnej**. W międzyczasie, aby zwalczać obrót towarami podrobionymi w Internecie, administracje celne państw członkowskich i Komisja powinny – w stosownych przypadkach – wprowadzić odpowiednie przepisy, utworzyć w swoich organach celnych punkty kontaktowe i prowadzić wymianę najlepszych praktyk.

Działanie 3: Konfiskata mienia pochodzącego z działalności przestępczej

Aby pozbawić siatki przestępcze zachęt finansowych, państwa członkowskie muszą robić wszystko, co w ich mocy, w celu przechwytywania, zamrażania i konfiskowania aktywów pochodzących z działalności przestępczej oraz zarządzania nimi i dbania o to, by nie trafiały z powrotem w ręce przestępców.

---

[9] Artykuł 88 ust. 2 lit. b) TFUE oraz decyzja Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej.

[10] Konkluzje Rady 15358/10 w sprawie opracowania i realizacji cyklu polityki unijnej dotyczącej poważnej i zorganizowanej przestępczości międzynarodowej.

W tym celu Komisja przedłoży w 2011 r. projekt **przepisów** rozszerzających unijne ramy prawne dotyczące **konfiskaty**[11]. Na jego podstawie możliwe będzie w szczególności dokonywanie konfiskaty mienia osób trzecich[12], rozszerzenie kompetencji w zakresie konfiskaty[13] oraz ułatwienie wzajemnego uznawania przez państwa członkowskie nakazów konfiskaty bez uprzedniego wyroku skazującego[14].

Państwa członkowskie są zobowiązane[15] do utworzenia najpóźniej w 2014 r. **biur ds. odzyskiwania mienia** wyposażonych w niezbędne środki i kompetencje oraz merytorycznie przygotowanych i zdolnych do wymiany informacji. Komisja opracuje do 2013 r. wspólne wskaźniki, na podstawie których państwa członkowskie będą następnie oceniać działalność tych biur. Ponadto państwa członkowskie powinny także do 2014 r. dokonać niezbędnych zabiegów organizacyjnych, takich jak utworzenie biur ds. zarządzania mieniem, by zagwarantować, że zamrożone mienie nie straci na wartości do momentu jego ostatecznej konfiskaty. Równocześnie Komisja przedłoży do 2013 r. wytyczne dotyczące najlepszych praktyk w zakresie zapobiegania odzyskiwaniu skonfiskowanego mienia przez grupy przestępcze.

CEL 2: Zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów

Zagrożenie ze strony terroryzmu jest nadal poważne i stale się zmienia[16]. Jak to widać na przykładzie zamachów w Bombaju w 2008 r., próby ataku na samolot lecący z Amsterdamu do Detroit w dzień Bożego Narodzenia 2009 r. i udaremnionych zamachów w kilku państwach członkowskich w ostatnim czasie, organizacje terrorystyczne dostosowują i unowocześniają swoje strategie. Obecnie zagrożenie stanowią zarówno zorganizowane grupy terrorystyczne, jak i osoby działające w pojedynkę, które reprezentują radykalne poglądy ukształtowane przez ekstremistyczną propagandę, a swoją działalność opierają na materiałach szkoleniowych dostępnych w Internecie. Nasze strategie zwalczania terroryzmu muszą również ewoluować, aby stale wyprzedzać o krok to zagrożenie, przy zastosowaniu spójnego podejścia europejskiego, w tym działań prewencyjnych[17]. Ponadto UE powinna w dalszym ciągu wskazywać elementy infrastruktury krytycznej i realizować plany dotyczące ochrony

---

11 Decyzja ramowa 2001/500/WSiSW w sprawie prania brudnych pieniędzy i konfiskaty.

12 Konfiskata w stosunku do osób trzecich oznacza konfiskatę mienia, które zostało przeniesione na osoby trzecie przez osobę, wobec której jest prowadzone śledztwo lub która została skazana.

13 Rozszerzenie prawa do konfiskaty oznacza, że konfiskowane może być mienie wykraczające poza korzyści majątkowe pochodzące bezpośrednio z przestępstwa bez konieczności wykazania związku między domniemanymi zyskami pochodzącymi z przestępstwa a popełnieniem konkretnego przestępstwa.

14 Procedura konfiskaty bez uprzedniego wyroku skazującego umożliwia zamrożenie i konfiskatę mienia, nawet jeżeli jego właściciel nie został skazany przez sąd w sprawie karnej.

15 Decyzja Rady 2007/845/WSiSW nakłada na każde państwo członkowskie obowiązek utworzenia na swoim terytorium co najmniej jednego biura ds. odzyskiwania mienia.

16 Najświeższe dane znajdują się w sprawozdaniu przygotowanym przez Europol za rok 2010, dotyczącym sytuacji i tendencji w zakresie terroryzmu (TESAT).

17 Strategia UE w dziedzinie walki z terroryzmem, dokument 14469/4/05 z listopada 2005 r., określa cztery kierunki działań obejmujące zapobieganie, ochronę, ściganie i reagowanie. Bardziej szczegółowe omówienie – zob.: „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania" – COM(2010) 386.

zasobów niezbędnych dla funkcjonowania społeczeństwa i gospodarki, w tym sektora transportu oraz energetyki (wytwarzanie i przesył energii)[18].

Pierwszoplanową rolę w drodze do osiągnięcia tego celu odgrywają państwa członkowskie podejmujące skoordynowane i skuteczne działania przy pełnym wsparciu Komisji i pomocy ze strony Koordynatora UE ds. Zwalczania Terroryzmu.

Działanie 1: Wzmocnienie pozycji społeczeństwa w zapobieganiu radykalizacji postaw i werbowaniu terrorystów

Radykalizacji postaw, która może prowadzić do aktów terroryzmu, można najlepiej zapobiec, podejmując działania jak najbliżej osób najbardziej podejrzanych w najbardziej narażonych na to zjawisko środowiskach. Wymaga to ścisłej współpracy z władzami lokalnymi i społeczeństwem obywatelskim oraz włączenia w procesy decyzyjne wiodących grup z najbardziej narażonych środowisk. Większość działań przeciwko radykalizacji postaw i werbowaniu terrorystów jest podejmowana na szczeblu państw członkowskich i tak też powinno pozostać.

Kilka państw członkowskich opracowuje programy zadaniowe w tej dziedzinie, a niektóre miasta w UE posiadają własne koncepcje i strategie prewencyjne oparte na społeczności lokalnej. Ponieważ inicjatywy te były często skuteczne, Komisja będzie nadal wspierać rozpowszechnianie takich doświadczeń[19].

Po pierwsze, Komisja we współpracy z Komitetem Regionów zaangażuje się w utworzenie do 2011 r. **unijnej sieci na rzecz uświadamiania na temat radykalizacji**, której będzie towarzyszyło forum internetowe oraz seria ogólnoeuropejskich konferencji, która będzie służyć do gromadzenia doświadczeń, wiedzy i dobrych praktyk w celu zwiększenia świadomości na temat radykalizacji oraz technik komunikacji w celu udaremnienia rozpowszechniania się idei terrorystycznych. Do sieci tej należeć będą osoby odpowiedzialne za wyznaczanie kierunków polityki, pracownicy organów ścigania i służb bezpieczeństwa, prokuratorzy, władze lokalne, pracownicy naukowi, eksperci terenowi i organizacje społeczeństwa obywatelskiego, w tym stowarzyszenia ofiar. Państwa członkowskie powinny wykorzystywać idee wypracowywane przez sieć do tworzenia realnych i wirtualnych forów dla otwartych dyskusji społecznych, które dawałyby osobom cieszącym się autorytetem i zaufaniem oraz opiniotwórczym liderom możliwość przekazywania pozytywnych przesłań będących przeciwwagą dla idei terrorystycznych. Komisja będzie również wspierać pracę organizacji społeczeństwa obywatelskiego, które ujawniają, tłumaczą i obalają brutalną propagandę ekstremistyczną w Internecie.

Po drugie, Komisja zorganizuje w 2012 r. **konferencję ministerialną** na temat zapobiegania radykalizacji i werbowaniu, na której państwa członkowskie będą miały okazję

---

[18] Dyrektywa w sprawie europejskiej infrastruktury krytycznej (2008/114/WE) jako część szerszego europejskiego programu ochrony infrastruktury krytycznej, którego zakres wykracza poza ochronę przed zagrożeniem ze strony terroryzmu.

[19] W ramach strategii UE w walce z radykalizacją postaw i werbowaniem terrorystów (CS/2008/15175) Komisja wspiera prace badawcze i tworzenie europejskiej sieci ekspertów ds. radykalizacji w celu zbadania zjawiska radykalizacji i werbowania terrorystów. Poza tym Komisja wspiera projekty kierowane przez państwa członkowskie, przykładowo projekty dotyczące współdziałania policji i społeczności lokalnej oraz komunikacji i radykalizacji w więzieniach, przekazała około 5 mln EUR na projekty na rzecz pomocy ofiarom oraz wspiera działalność sieci stowarzyszeń ofiar terroryzmu.

zaprezentowania przykładów swoich skutecznych działań przeciwko ideologiom ekstremistycznym.

Po trzecie, w kontekście tych inicjatyw i dyskusji Komisja opracuje **podręcznik działań i doświadczeń** mający wesprzeć działania państw członkowskich, począwszy od oddolnego zapobiegania radykalizacji, a skończywszy na rozbijaniu kanałów werbunku oraz działaniu na rzecz rehabilitacji i kreowania postaw negatywnych wobec terroryzmu.

Działanie 2: Odcięcie terrorystów od źródeł finansowania i materiałów oraz śledzenie dokonywanych przez nich transakcji

W 2011 r. Komisja rozważy przedłożenie zgodnie z art. 75 Traktatu dokumentu ramowego w sprawie środków administracyjnych dotyczących zamrażania aktywów finansowych w celu zwalczania terroryzmu i związanych z nim działań. Należy priorytetowo realizować plany działania UE dotyczące uniemożliwiania dostępu do materiałów wybuchowych (2008 r.) oraz do substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRN) (2009 r.) poprzez działania ustawodawcze i nieustawodawcze. Obejmuje to również przyjęcie rozporządzenia dotyczącego ograniczenia ogólnego dostępu do prekursorów chemicznych wykorzystywanych do produkcji materiałów wybuchowych. Odpowiedni wniosek został przedłożony przez Komisję w 2010 r. Dotyczy to także utworzenia europejskiej sieci jednostek organów ścigania wyspecjalizowanych w sprawach dotyczących CBRN, co ma zapewnić uwzględnienie przez państwa członkowskie zagrożeń wynikających z CBRN w planach przygotowywanych na szczeblu krajowym. Kolejnym działaniem będzie utworzenie przy Europolu systemu wczesnego ostrzegania dla egzekwowania prawa w przypadku zdarzeń związanych z substancjami CBRN. Działania te wymagają ścisłej koordynacji z państwami członkowskimi i powinny opierać się również, w stosownych przypadkach, na partnerstwach publiczno-prywatnych. Aby ograniczyć do minimum ryzyko wejścia przez organizacje terrorystyczne i podmioty państwowe w posiadanie substancji, które mogłyby zostać wykorzystane do produkcji materiałów wybuchowych i broni masowego rażenia (substancji biologicznych, chemicznych lub jądrowych), UE powinna zaostrzyć swój system kontroli wywozu produktów podwójnego zastosowania i jego egzekwowanie na granicach UE oraz w wymiarze międzynarodowym.

Po podpisaniu ze Stanami Zjednoczonymi Umowy w sprawie programu śledzenia środków finansowych należących do terrorystów (TFTP) Komisja opracuje w 2011 r. **politykę UE w zakresie pozyskiwania i analizy danych z komunikatów finansowych** zarejestrowanych na terenie UE**.**

Działanie 3: Ochrona transportu

Komisja będzie dalej rozwijać unijną politykę bezpieczeństwa transportu lotniczego i morskiego na podstawie ciągłej oceny ryzyk i zagrożeń. Weźmie ona przy tym pod uwagę postęp, jaki dokonał się w zakresie procesów i technologii badań nad bezpieczeństwem, wykorzystując przy tym funkcjonujące programy UE, takie jak Galileo oraz inicjatywa GMES[20] służąca obserwacji Ziemi. Komisja chce zdobyć poparcie opinii publicznej, starając się stale udoskonalać równowagę pomiędzy jak największym stopniem bezpieczeństwa i

[20] GMES (ang. *Global Monitoring for Environment and Security*) – Globalny monitoring środowiska i bezpieczeństwa.

komfortu podróży, obniżaniem kosztów oraz ochroną sfery prywatnej i zdrowia. Będzie się ona również angażować na rzecz dalszego wzmacniania systemu kontroli i egzekwowania przepisów, w tym nadzorowania obsługi ładunków. Istotna jest współpraca międzynarodowa, która może wnieść wkład w podniesienie światowych norm bezpieczeństwa, a jednocześnie zapewnić efektywne wykorzystanie zasobów i ograniczyć zbędne podwójne kontrole bezpieczeństwa.

Bardziej aktywne europejskie podejście do obszernego i kompleksowego zagadnienia, jakim jest **bezpieczeństwo transportu lądowego**, w szczególności w zakresie bezpieczeństwa przewozów pasażerskich, jest możliwe i uzasadnione[21]. Komisja zamierza rozszerzyć aktualne prace nad bezpieczeństwem transportu miejskiego o działania w zakresie (a) lokalnego i regionalnego transportu szynowego oraz (b) kolei dużych prędkości, w tym odpowiedniej do tego infrastruktury. Działania na szczeblu UE ograniczały się dotychczas do wymiany informacji i najlepszych praktyk z uwagi na zasadę pomocniczości i z powodu braku międzynarodowej organizacji porównywalnej z Międzynarodową Organizacją Morską lub Międzynarodową Organizacją Lotnictwa Cywilnego, która wymagałaby skoordynowanego podejścia europejskiego. Komisja jest zdania, że biorąc pod uwagę wcześniejsze doświadczenia w zakresie bezpieczeństwa lotnictwa i transportu morskiego, pierwszym krokiem do dalszego działania powinno być zbadanie możliwości utworzenia stałego komitetu do spraw bezpieczeństwa transportu lądowego, któremu przewodniczyłaby Komisja i który składałby się z ekspertów z dziedziny transportu i egzekwowania prawa, oraz utworzenia forum wymiany opinii z zainteresowanymi podmiotami publicznymi i prywatnymi. W świetle najnowszych wydarzeń przyspieszono dotychczasowe działania w celu poprawy i zaostrzenia procedur monitorowania ładunków lotniczych będących w trakcie tranzytu z państw trzecich.

Kwestie bezpieczeństwa transportu zostaną omówione szczegółowo w komunikacie w sprawie polityki bezpieczeństwa transportu, którego opublikowanie planowane jest na 2011 r.

CEL 3: Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni

Bezpieczeństwo sieci informatycznych jest jednym z zasadniczych warunków dobrze funkcjonującego społeczeństwa informacyjnego. Uznano to w opublikowanej niedawno Europejskiej agendzie cyfrowej[22], która jest poświęcona tematom związanym z cyberprzestępczością, bezpieczeństwem cybernetycznym, bezpieczeństwem w Internecie i ochroną prywatności jako głównymi elementami budowania zaufania i bezpieczeństwa użytkowników sieci. Szybki rozwój i zastosowanie nowych technologii informacyjnych przyczyniły się również do powstania nowych form działalności przestępczej. Cyberprzestępczość jest zjawiskiem ogólnoświatowym, które powoduje znaczne szkody na rynku wewnętrznym w UE. Internet nie zna granic, natomiast jurysdykcja w zakresie ścigania przestępstw cybernetycznych nadal zatrzymuje się na granicach państwowych. Państwa członkowskie powinny połączyć swoje działania na szczeblu UE. Centrum zwalczania przestępczości związanej z technologią zaawansowaną (ang. *High Tech Crime Centre*), działające przy Europolu, odgrywa już znaczącą rolę w koordynacji działań na rzecz egzekwowania prawa, niezbędne są jednak dalsze działania.

---

21 Rada Europejska, marzec 2004 r., Deklaracja w sprawie zwalczania terroryzmu.

22 COM(2010) 245.

Działanie 1: Budowa zdolności w zakresie egzekwowania prawa i sądownictwa

Do 2013 r. UE utworzy w ramach istniejących struktur **centrum ds. walki z cyberprzestępczością**, które umożliwi państwom członkowskim i instytucjom UE budowanie zdolności operacyjnych i analitycznych do prowadzenia dochodzeń oraz pogłębienie współpracy z partnerami międzynarodowymi[23]. Centrum to wniesie wkład w poprawę oceny i nadzorowania istniejących środków prewencyjnych i dochodzeniowych, w tworzenie działań mających na celu szkolenie i uświadamianie organów ścigania i sądownictwa, w nawiązanie współpracy z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz połączenie z siecią krajowych/rządowych zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (ang. *Computer Emergency Response Teams*, CERT). Centrum ds. walki z cyberprzestępczością powinno stać się centralnym miejscem zwalczania cyberprzestępczości w UE.

Na szczeblu krajowym państwa członkowskie powinny zapewnić jednolite normy dla funkcjonariuszy policji, sędziów, prokuratorów i ekspertów z dziedziny kryminalistyki prowadzących działania dochodzeniowo-śledcze w sprawach związanych z cybeprzestępczością. Zaleca się państwom członkowskim, by w porozumieniu z Eurojustem, CEPOL-em i Europolem do 2013 r. rozwinęły swoje krajowe zdolności w zakresie uwrażliwiania i kształcenia na temat cyberprzestępczości i aby utworzyły centra doskonałości na szczeblu krajowym lub w partnerstwie z innymi państwami członkowskimi. Centra te powinny ściśle współpracować ze szkołami wyższymi i przemysłem.

Działanie 2: Współpraca z przemysłem w celu wzmacniania pozycji obywateli i ich ochrony

Wszystkie państwa członkowskie powinny zadbać o to, by każdy obywatel bez utrudnień mógł **złożyć zawiadomienie o popełnieniu cyberprzestępstwa**. Po dokonaniu oceny takiej informacji trafiałaby ona do krajowej lub – w stosownych przypadkach – europejskiej platformy ostrzegania przed cyberprzestępstwami. Opierając się na wartościowych pracach w ramach programu „Bezpieczniejszy Internet", państwa członkowskie powinny zadbać również o to, by obywatele mieli łatwy dostęp do informacji na temat zagrożeń w sieci i do podstawowych środków ostrożności, których podjęcie jest niezbędne. Informacje te powinny zawierać wskazówki, jak chronić swoją prywatność w Internecie, jak wykrywać i zgłaszać nagabywanie dzieci dla celów seksualnych, jak wyposażyć swój komputer w podstawowe oprogramowanie antywirusowe i ochrony dostępu, jak zarządzać hasłami dostępu i jak wykrywać *phishing*, *pharming* i inne rodzaje ataków. Komisja utworzy w 2013 r. działającą w czasie rzeczywistym centralną bazę zawierającą wspólne zasoby i przykłady najlepszych praktyk ze strony państw członkowskich i przemysłu.

Należy również wzmocnić współpracę pomiędzy sektorem publicznym a sektorem prywatnym na szczeblu europejskim poprzez europejskie partnerstwo publiczno-prywatne na rzecz odporności kluczowej infrastruktury informacyjnej (ang. *European Public-Private Partnership for Resilience* – EP3R). Należy podejmować dalsze innowacyjne środki i instrumenty w celu poprawy bezpieczeństwa, w tym bezpieczeństwa kluczowej infrastruktury, oraz odporności sieci i infrastruktury informacyjnej. EP3R powinno także obejmować partnerów z krajów trzecich, aby poprawić skuteczność światowego zarządzania ryzykiem w zakresie sieci informatycznych.

[23] Komisja ukończy studium wykonalności dla tego centrum w 2011 r.

Zwalczanie nielegalnych treści w Internecie, w tym haseł podburzających do terroryzmu, powinno odbywać się w oparciu o wytyczne dotyczące współpracy, zawierające autoryzowane procedury zgłaszania i usuwania takich treści. Komisja zamierza opracować takie wytyczne wraz z dostawcami usług internetowych, organami ścigania i organizacjami nienastawionymi na zysk do 2011 r. Komisja będzie zachęcać do kontaktów i interakcji pomiędzy tymi podmiotami, promując korzystanie z platformy internetowej o nazwie: *Contact Initiative against Cybercrime for Industry and Law Enforcement* (Inicjatywa kontaktowa przeciwko cyberprzestępczości dla przemysłu i egzekwowania prawa).

Działanie 3: Poprawa zdolności do reagowania na ataki cybernetyczne

Konieczne jest podjęcie szeregu kroków w celu poprawy skuteczności zapobiegania atakom i zakłóceniom cybernetycznym, ich wykrywania i niezwłocznego reagowania na nie. Po pierwsze, każde państwo członkowskie oraz same instytucje UE powinny do 2012 r. dysponować własnym dobrze funkcjonującym zespołem **CERT**. Ważne jest, by po ich utworzeniu wszystkie zespoły CERT współpracowały z organami ścigania w zakresie prewencji i reagowania. Po drugie, państwa członkowskie powinny do 2012 r. utworzyć wspólną sieć krajowych/rządowych CERT, by zwiększyć gotowość Europy. Działanie to walnie przyczyni się do opracowania do 2013 r. – przy wsparciu ze strony Komisji i ENISA – europejskiego systemu ostrzegania i wymiany informacji (ang. *European Information Sharing and Alert System* – EISAS) i przedstawienia go szerszej opinii publicznej oraz do utworzenia sieci punktów kontaktowych pomiędzy właściwymi jednostkami a państwami członkowskimi. Po trzecie, państwa członkowskie powinny we współpracy z ENISA opracować krajowe plany awaryjne i przeprowadzać na szczeblu krajowym i europejskim regularne ćwiczenia w zakresie obrony przed atakami cybernetycznymi i odzyskiwania danych w przypadku awarii. ENISA będzie wspierać te działania w celu podniesienia standardów dla zespołów CERT w Europie.

CEL 4: Poprawa bezpieczeństwa poprzez zarządzanie granicami

Po wejściu w życie traktatu lizbońskiego łatwiej jest Unii Europejskiej zadbać o synergię pomiędzy różnymi podejściami do zarządzania granicami w odniesieniu do przepływu osób i towarów w duchu solidarności i podziału odpowiedzialności[24]. W dziedzinie przepływu osób UE może traktować zarządzanie migracjami i walkę z przestępczością jako dwa bliźniacze cele zintegrowanej strategii zarządzania granicami. Strategia ta opiera się na trzech filarach:

- szerszym zastosowaniu nowych technologii do celów kontroli granicznych (systemu informacyjnego Schengen drugiej generacji (SIS II), wizowego systemu informacyjnego (VIS), systemu wjazdu/wyjazdu i programu rejestrowania podróżnych);

- szerszym zastosowaniu nowych technologii do ochrony granic (europejskiego systemu nadzoru granic, EUROSUR) przy wykorzystaniu usług programu GMES i stopniowym tworzeniu wspólnego środowiska wymiany informacji dla obszarów morskich UE[25]; oraz

[24] Artykuł 80 TFUE.

[25] Komunikat Komisji „W kierunku integracji nadzoru morskiego: Wspólny mechanizm wymiany informacji dla obszarów morskich UE", COM(2009) 538.

- usprawnieniu koordynacji działań państw członkowskich poprzez Frontex.

W dziedzinie swobodnego przepływu towarów dzięki zmianie w zakresie bezpieczeństwa do Wspólnotowego kodeksu celnego[26], której dokonano w 2005 r., granice stały się bezpieczniejsze i bardziej przepuszczalne dla towarów niebudzących wątpliwości. Wszelkie ładunki wwożone na terytorium UE są ze względów bezpieczeństwa poddawane analizie ryzyka, która opiera się na wspólnych kryteriach i normach w zakresie ryzyka. W ten sposób istniejące zasoby są wykorzystywane bardziej efektywnie, gdyż można je skoncentrować na ładunkach, które stanowią potencjalne ryzyko. System opiera się na zasadzie uprzedniego informowania o planowanym ruchu towarów przez podmioty uczestniczące w transakcji handlowej, utworzeniu wspólnych ram zarządzania ryzykiem oraz koncepcji „upoważnionego przedsiębiorcy", która ma mieć zastosowanie do wszystkich towarów, które są wwożone do UE i wywożone z UE. Instrumenty te uzupełniają się wzajemnie i tworzą kompleksowy system, który podlega dalszemu rozwojowi, by uporać się z coraz bardziej wyrafinowanymi organizacjami przestępczymi, z którymi państwa członkowskie pojedynczo nie mogą sobie poradzić.

Działanie 1: Wykorzystanie pełnego potencjału EUROSUR

Komisja przedstawi w 2011 r. wniosek legislacyjny w sprawie **ustanowienia EUROSUR** jako wkład w bezpieczeństwo wewnętrzne i zwalczanie przestępczości. Dzięki EUROSUR organy państw członkowskich uzyskają możliwość wymiany informacji operacyjnych związanych z ochroną granic oraz współpracy między sobą i z agencją Frontex na płaszczyźnie taktycznej, operacyjnej i strategicznej[27]. EUROSUR będzie korzystać z nowych technologii rozwijanych w ramach projektów badawczych finansowanych ze środków UE, takich jak obrazy satelitarne do wykrywania i śledzenia celów na granicach morskich, np. do śledzenia szybkich łodzi przewożących narkotyki do UE.

W ostatnich latach zapoczątkowano dwie większe inicjatywy w zakresie współpracy operacyjnej na granicach morskich – jedną z nich była inicjatywa dotycząca handlu ludźmi i przemytu ludzi pod patronatem Frontex, a drugą – inicjatywa dotycząca przemytu narkotyków w ramach MAOC-N[28] i CeCLAD-M[29]. W 2011 r. UE rozpocznie projekt pilotażowy na swoich południowych i południowo-zachodnich granicach, który będzie częścią zintegrowanych i operacyjnych działań na granicach morskich Unii. W projekt będą zaangażowane oba ww. ośrodki, Komisja, Frontex i Europol. Celem tego projektu pilotażowego będzie wytworzenie synergii w zakresie danych dotyczących analizy i nadzorowania ryzyka w obszarach będących przedmiotem wspólnego zainteresowania dotyczących różnych rodzajów zagrożeń, takich jak narkotyki i przemyt ludzi[30].

---

26 Rozporządzenie Rady (WE) nr 648/2005 zmieniające rozporządzenie Rady (WE) nr 2913/92 ustanawiające Wspólnotowy Kodeks Celny.

27 Wnioski Komisji dotyczące stworzenia systemu EUROSUR oraz stworzenia wspólnego mechanizmu wymiany informacji dla obszarów morskich UE znajdują się w dokumentach, odpowiednio, COM (2008) 68 oraz COM(2009) 538. Niedawno został przyjęty sześcioetapowy plan działania na rzecz stworzenia CISE – COM(2010) 584.

28 MAOC-N – Morskie Centrum Analiz i Operacji ds. Zwalczania Narkotyków.

29 CeCLAD-M – Ośrodek Koordynacji Walki z Narkotykami na Morzu Śródziemnym.

30 Projekt ten uzupełni inne projekty ukierunkowane na zintegrowane bezpieczeństwo morskie, takie jak BlueMassMed oraz Marsuno, których celem jest optymalizacja efektywności nadzoru morskiego na Morzu Śródziemnym, Atlantyku i basenach morskich Europy Północnej.

Działanie 2: Zwiększenie wkładu Frontexu w zwalczanie przestępczości na granicach zewnętrznych

W trakcie swojej pracy operacyjnej Frontex natrafia na ważne informacje na temat członków grup przestępczych działających w siatkach przemytniczych. Aktualnie informacji tych nie można jednak wykorzystać do analizy ryzyka lub lepszego ukierunkowania przyszłych wspólnych operacji. Odpowiednie informacje na temat domniemanych przestępców nie docierają poza tym do właściwych organów krajowych ani do Europolu, gdzie mogłyby posłużyć do dalszych działań śledczych. Również Europol nie może udostępniać informacji znajdujących się w jego aktach analitycznych. W oparciu o dotychczasowe doświadczenia i w kontekście ogólnego podejścia UE do zarządzania informacjami[31] Komisja jest zdania, że umożliwienie Frontexowi przetwarzania i wykorzystywania tych informacji – w ograniczonym zakresie i zgodnie z jasno sprecyzowanymi przepisami w zakresie zarządzania danymi osobowymi – będzie stanowiło znaczący wkład w rozbijanie organizacji przestępczych. Nie powinno to jednak prowadzić do dublowania się zadań wykonywanych przez Frontex i Europol.

Od 2011 r. Komisja będzie przedkładać na koniec każdego roku sprawozdanie przygotowywane przy uwzględnieniu informacji z Frontexu i Europolu w sprawie określonych rodzajów przestępczości transgranicznej, takiej jak handel ludźmi, przemyt ludzi i przemyt nielegalnych towarów. To coroczne sprawozdanie posłuży jako podstawa do oceny potrzeb Frontexu w kontekście jego wspólnych operacji, jak również wspólnych operacji policji, organów celnych i innych wyspecjalizowanych organów ścigania, które będą prowadzone od roku 2012.

Działanie 3: Wspólne zarządzanie ryzykiem w odniesieniu do przepływu towarów przez zewnętrzne granice UE

W ostatnich latach miały miejsce znaczące zmiany prawne i strukturalne, mające na celu poprawę bezpieczeństwa międzynarodowych łańcuchów dostaw i przepływu towarów przez zewnętrzne granice UE. Wspólne ramy zarządzania ryzykiem wdrożone przez organy celne obejmują prowadzenie ciągłych kontroli elektronicznych danych handlowych przed wwozem (i wywozem) w celu określenia zagrożeń dla bezpieczeństwa Unii i jej obywateli oraz odpowiednie działania w celu ograniczenia tych zagrożeń. Ramy te przewidują również możliwość stosowania bardziej intensywnych kontroli w dziedzinach określonych jako priorytetowe, włączając w to politykę handlową i ryzyko finansowe. Elementem ram jest również systematyczna wymiana informacji na temat ryzyka na szczeblu UE.

Wyzwaniem na nadchodzące lata będzie zadbanie o to, by zarządzanie ryzykiem, związana z tym analiza ryzyka oraz kontrole przeprowadzane na podstawie oceny ryzyka odbywały się we wszystkich państwach członkowskich na takim samym, wysokim poziomie. Aby ograniczyć zakres wspólnego ryzyka, Komisja – oprócz opracowania sprawozdania rocznego w sprawie przemytu nielegalnych towarów – przeprowadzi również ocenę informacji celnych na szczeblu UE. Gromadzenie informacji na szczeblu unijnym powinno zostać wykorzystane do wzmocnienia bezpieczeństwa granic. Aby uzyskać wymagany poziom bezpieczeństwa poprzez środki celne podejmowane na granicach zewnętrznych, Komisja będzie w 2011 r.

[31] Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości – COM(2010) 385.

pracowała nad możliwościami **poprawy zdolności w zakresie określania ryzyka i jego analizy na szczeblu unijnym**, i przedłoży w stosownych przypadkach odpowiednie wnioski.

Działanie 4: Poprawa współpracy między organami krajowymi

Do końca 2011 r. państwa członkowskie powinny rozpocząć prace nad **analizami wspólnego ryzyka**. Powinny one objąć wszystkie właściwe organy odgrywające istotną rolę w sprawach bezpieczeństwa, tzn. policję, straż graniczną i organy celne, których zadaniem będzie identyfikowanie newralgicznych punktów oraz wielokrotnych i przekrojowych zagrożeń na granicach zewnętrznych, np. powtarzającego się przemytu ludzi i narkotyków z tego samego regionu na tych samych przejściach granicznych. Analizy te powinny uzupełniać sprawozdania roczne Komisji w sprawie przestępczości transgranicznej, uwzględniające informacje z Frontexu i Europolu. Do końca 2010 r. Komisja zakończy opracowywanie analizy dotyczącej najlepszych praktyk w zakresie współpracy pomiędzy strażą graniczną a administracją celną na zewnętrznych granicach UE i podejmie rozważania nad najlepszym sposobem ich rozpowszechniania. W 2012 r. Komisja przedstawi propozycje dotyczące **poprawy koordynacji kontroli granicznych** przeprowadzanych przez różne organy krajowe (policję, straż graniczną i służby celne). Oprócz tego Komisja opracuje do 2014 r. wraz z Frontexem, Europolem i Europejskim Urzędem Wsparcia w dziedzinie Azylu minimalne normy i najlepsze praktyki dla współpracy między różnymi organami. Znajdą one w szczególności zastosowanie we wspólnej analizie ryzyka, wspólnych dochodzeniach, wspólnych operacjach i wymianie informacji.

CEL 5: Zwiększenie odporności Europy na kryzysy i katastrofy

Unia Europejska jest narażona na szereg potencjalnych kryzysów i katastrof, jak na przykład klęski żywiołowe związane ze zmianą klimatu, kryzysy spowodowane przez ataki terrorystyczne i cybernetyczne na infrastrukturę krytyczną, wrogie lub nieumyślne uwolnienie czynników chorobotwórczych i patogenów, nagłe wybuchy epidemii grypy lub awarie infrastruktury. W świetle tego rodzaju zagrożeń rozciągających się na różne sektory konieczna jest poprawa efektywności i spójności stosowanych od dawna praktyk w dziedzinie zarządzania kryzysowego i zarządzania katastrofami. Wymaga to zarówno solidarności w reagowaniu na wypadek zagrożenia, jak i odpowiedzialności w działaniach zapobiegawczych i przygotowawczych, przy czym główny nacisk należy położyć na poprawę oceny ryzyka i zarządzania ryzykiem na szczeblu UE w odniesieniu do wszystkich potencjalnych zagrożeń.

Działanie 1: Pełne zastosowanie klauzuli solidarności

Klauzula solidarności zawarta w traktacie lizbońskim[32] nakłada na UE i jej państwa członkowskie obowiązek udzielania sobie wzajemnej pomocy, jeżeli jakiekolwiek państwo członkowskie stanie się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej lub katastrofy spowodowanej przez człowieka. Realizacja tej klauzuli ma przysłużyć się temu, by UE była lepiej zorganizowana i bardziej skuteczna w zarządzaniu kryzysowym w odniesieniu zarówno do zapobiegania kryzysom, jak i reagowania na nie. Wspólnym zadaniem UE będzie teraz **praktyczna realizacja klauzuli solidarności** w oparciu o przekrojowy wniosek Komisji i Wysokiego Przedstawiciela, który zostanie przedłożony w 2011 r.

[32] Artykuł 222 TFUE.

Działanie 2: Podejście do oceny zagrożenia i ryzyka przy uwzględnieniu wszystkich rodzajów zagrożenia

Do końca 2010 r. Komisja opracuje wspólnie z państwami członkowskimi unijne wytyczne dotyczące **oceny ryzyka** i jego mapowania w zakresie zarządzania katastrofami, opierając się na podejściu ukierunkowanym na wiele rodzajów zagrożenia i ryzyka, które zasadniczo uwzględnia wszystkie klęski żywiołowe oraz katastrofy spowodowane przez człowieka. Do końca 2011 r. państwa członkowskie powinny opracować swoje krajowe strategie zarządzania ryzykiem, w tym analizy ryzyka. Na tej podstawie Komisja przygotuje do końca 2012 r. ponadsektorowy przegląd najważniejszych ryzyk naturalnych i tych wywoływanych przez człowieka, z którymi UE może być skonfrontowana w przyszłości[33]. Ponadto planowana na 2011 r. inicjatywa Komisji dotycząca bezpieczeństwa zdrowotnego będzie próbą wzmocnienia koordynacji zarządzania ryzykiem w UE. Poprawi ona również istniejące struktury i mechanizmy w dziedzinie zdrowia publicznego.

Jeśli chodzi o **ocenę zagrożenia**, Komisja będzie wspierać działania na rzecz lepszego zrozumienia różnych definicji stopni zagrożenia oraz poprawy komunikacji w przypadku zmiany tych stopni. Wzywa się państwa członkowskie do opracowania w 2012 r. własnych ocen zagrożenia w odniesieniu do ataków terrorystycznych i innych złowrogich zagrożeń. Od 2013 r. Komisja we współpracy z koordynatorem UE ds. zwalczania terroryzmu i państwami członkowskimi będzie w regularnych odstępach czasu przygotowywać przeglądy aktualnych zagrożeń na podstawie ocen krajowych.

Do 2014 r. UE powinna opracować spójną **politykę zarządzania ryzykiem**, która włączy ocenę zagrożenia i ocenę ryzyka do procedur podejmowania decyzji.

Działanie 3: Połączenie w sieć różnych ośrodków służących obserwacji położenia

Aby reagowanie na stany kryzysowe było skuteczne i skoordynowane, konieczna jest możliwość wyrobienia sobie w sposób szybki dokładnego i kompleksowego przeglądu sytuacji. Ze wszystkich stosownych źródeł należy pozyskiwać informacje na temat sytuacji wewnątrz Unii i poza nią, a następnie je analizować, oceniać i wymieniać się nimi z państwami członkowskimi oraz jednostkami operacyjnymi i właściwymi merytorycznie służbami w instytucjach unijnych. Poprzez całkowite usieciowienie bezpiecznych urządzeń, właściwe wyposażenie i odpowiednio przeszkolony personel UE może **stworzyć zintegrowaną strategię na wypadek sytuacji kryzysowej w oparciu o wspólną ocenę sytuacji**.

Opierając się na istniejących możliwościach i wiedzy fachowej, Komisja wzmocni do 2012 r. powiązania pomiędzy sektorowymi systemami wczesnego ostrzegania i mechanizmami współpracy kryzysowej[34], między innymi w takich dziedzinach jak opieka zdrowotna, ochrona ludności, monitorowanie zagrożeń jądrowych i terroryzm, korzystając przy tym z programów operacyjnych UE. Wniesie to wkład w poprawę powiązań z agencjami UE i Europejską Służbą Działań Zewnętrznych, w tym z Centrum Sytuacyjnym, i umożliwi lepszą

[33] Konkluzje Rady w sprawie wspólnotowych ram w zakresie zapobiegania katastrofom na terytorium UE, listopad 2009 r.

[34] Komisja będzie nadal wykorzystywać i rozwijać system ARGUS – zob. COM(2005) 662 – oraz związane z nim procedury na wypadek sytuacji kryzysowych obejmujących wielorakie zagrożenia i różne sektory oraz na potrzeby koordynacji w ramach wszystkich służb Komisji.

wymianę informacji i w razie potrzeby opracowywanie wspólnych sprawozdań z oceny zagrożenia i ryzyka w UE.

Skuteczna koordynacja pomiędzy unijnymi instytucjami, organami i agencjami wymaga spójnych ogólnych ram dla ochrony informacji niejawnych. Komisja zamierza zatem przedstawić w 2011 r. odpowiedni wniosek.

Działanie 4: Utworzenie europejskiego potencjału reagowania kryzysowego na wypadek katastrof

Unia Europejska powinna być w stanie reagować na katastrofy zarówno wewnątrz, jak i na zewnątrz UE. Doświadczenia z ostatnich wydarzeń pokazują, że wciąż jeszcze trzeba poprawić szybkość podejmowania działań i ich odpowiedniość, koordynację operacyjną i polityczną oraz eksponowania roli unijnego reagowania na wypadek klęsk w odniesieniu wewnętrznym, jak i zewnętrznym.

Zgodnie z niedawno przyjętą strategią reagowania na katastrofy[35] UE powinna **stworzyć europejski potencjał reagowania kryzysowego** w oparciu o wcześniej zadeklarowane zasoby państw członkowskich wykorzystywane do operacji unijnych oraz wcześniej ustalone plany awaryjne. Należy poprawić wydajność i opłacalność poprzez korzystanie ze wspólnych centrów logistycznych oraz uproszczenie i uściślenie procedur łączenia i współfinansowania środków transportu. W celu realizacji kluczowych sugestii Komisja przedłoży w 2011 r. wnioski legislacyjne.

3. REALIZACJA STRATEGII

Realizacja strategii bezpieczeństwa wewnętrznego UE w działaniu jest wspólnym obowiązkiem instytucji UE, państw członkowskich i unijnych agencji. Wymaga to uzgodnionego przez wszystkich procesu realizacji strategii z jasnym podziałem ról i zadań, przy czym Rada i Komisja, w ścisłym porozumieniu z Europejską Służbą Działań Zewnętrznych, są siłą napędową odpowiedzialną za postęp w kierunku osiągnięcia strategicznych celów. W szczególności Komisja będzie wspierać działalność Stałego Komitetu Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego (COSI), co pozwoli usprawnić i wzmocnić współpracę operacyjną oraz ułatwić koordynację działań właściwych organów państw członkowskich[36].

Realizacja

Priorytety muszą znajdować odzwierciedlenie zarówno w planowaniu operacyjnym agencji UE i państw członkowskich, jak i programach prac Komisji. Komisja zadba o to, by działania istotne dla bezpieczeństwa, w tym badania w dziedzinie bezpieczeństwa, polityka przemysłowa i projekty w ramach programów związanych z bezpieczeństwem wewnętrznym finansowanych przez UE, były spójne z celami strategicznymi. Badania w dziedzinie bezpieczeństwa będą nadal finansowane w oparciu o wieloletnie ramowe programy

[35] „Wzmacnianie europejskiej zdolności reagowania w przypadku klęsk i katastrof: rola ochrony ludności i pomocy humanitarnej – COM(2010) 600.

[36] Artykuł 71 TFUE; zob. też decyzja Rady 2010/131/UE w sprawie ustanowienia Stałego Komitetu Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego.

badawczo-rozwojowe. W celu zapewnienia pomyślnej realizacji Komisja powoła do życia wewnętrzną grupę roboczą. Do uczestnictwa zostanie zaproszona Europejska Służba Działań Zewnętrznych, co zapewni spójność z szerzej pojętą europejską strategią bezpieczeństwa i wytworzy synergię pomiędzy polityką wewnętrzną i zewnętrzną, włączając w to oceny ryzyka i zagrożenia. W tym samym celu również COSI i Komitet Polityczny i Bezpieczeństwa powinny współpracować i spotykać się regularnie.

Finansowanie UE, jakie może być niezbędne na okres 2011–2013, zostanie udostępnione w ramach aktualnego pułapu wieloletnich ram finansowych. Natomiast finansowanie bezpieczeństwa wewnętrznego na okres po roku 2013 zostanie przeanalizowane przez Komisję w ramach generalnej debaty na temat wszystkich wniosków, które zostaną przedłożone na ten okres. W ramach tej debaty Komisja rozważy możliwość utworzenia funduszu bezpieczeństwa wewnętrznego.

Monitorowanie i ocena

Komisja będzie wraz z Radą śledzić postępy w zakresie strategii bezpieczeństwa wewnętrznego w działaniu. W oparciu o informacje otrzymywane od państw członkowskich i agencji Komisja będzie przedkładać Parlamentowi Europejskiemu i Radzie coroczne sprawozdanie z realizacji strategii, wykorzystując przy tym w miarę możliwości istniejące procedury sprawozdawcze. W sprawozdaniu rocznym Komisja będzie omawiać najważniejsze postępy w drodze do osiągnięcia każdego z celów strategicznych i oceniać, czy działania na szczeblu unijnym i krajowym odniosły skutek, a także – w stosownych przypadkach – wystosowywać zalecenia. Sprawozdanie roczne będzie również zawierać załącznik opisujący stan bezpieczeństwa wewnętrznego. Przy jego opracowywaniu Komisja będzie się opierać na wkładzie ze strony właściwych agencji. Sprawozdanie mogłoby również corocznie służyć jako podstawa do dyskusji na temat bezpieczeństwa wewnętrznego na forum Parlamentu Europejskiego i Rady.

WNIOSKI KOŃCOWE

Nasz świat się zmienia, podobnie zmieniają się zagrożenia i wyzwania wokół nas. Reakcja ze strony Unii Europejskiej powinna ewoluować w ten sam sposób. Współpracując przy realizacji działań nakreślonych w tej strategii, jesteśmy na właściwej drodze. Jednocześnie nieuniknione jest to, że niezależnie od tego, jak silni i jak dobrze przygotowani będziemy, zagrożeń nie da się w całości wyeliminować. Dlatego właśnie tym ważniejsze jest, byśmy nasilili nasze działania.

Opierając się na traktacie lizbońskim jako nowej konstrukcji prawnej, strategia bezpieczeństwa wewnętrznego w działaniu powinna stać się wspólną agendą dla UE na najbliższe cztery lata. Jej sukces jest uzależniony nie tylko od połączonych starań wszystkich podmiotów UE, lecz również od współpracy ze światem zewnętrznym. Jedynie wspólnymi siłami i współpracując w celu realizacji tej strategii, państwa członkowskie, instytucje UE oraz organy i agencje mogą zapewnić prawdziwie skoordynowaną reakcję Europy na zagrożenia dla bezpieczeństwa w dzisiejszych czasach.

Załącznik: Zestawienie celów i działań

STRATEGIA BEZPIECZEŃSTWA WEWNĘTRZNEGO

CELE I DZIAŁANIA

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
CEL 1: Rozbijanie międzynarodowych siatek przestępczych		
Działanie 1: Wykrywanie i rozbijanie siatek przestępczych		
Wniosek w sprawie posługiwania się unijnymi danymi dotyczącymi przelotu pasażera	COM[37]	2011
Ewentualna zmiana przepisów UE dotyczących przeciwdziałania praniu pieniędzy, by umożliwić identyfikację właścicieli spółek i funduszy powierniczych	COM	2013
Wytyczne w sprawie korzystania z rejestru rachunków bankowych dla śledzenia przepływów środków finansowych pochodzących z przestępstw	COM	2012
Strategia w zakresie gromadzenia, analizy i wymiany informacji na temat przestępczych transakcji finansowych (w tym szkolenia)	COM wraz z MS i CEPOL	2012

[37] Wyjaśnienie do zastosowanych skrótów: Komisja Europejska (COM), państwa członkowskie (MS), Europejskie Kolegium Policyjne (CEPOL), Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), Morskie Centrum Analiz i Operacji ds. Zwalczania Narkotyków (MAOC-N), Ośrodek Koordynacji Walki z Narkotykami na Morzu Śródziemnym (CECLAD-M), Europejski Urząd Wsparcia w dziedzinie Azylu (EASO), Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (HR).

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
Większe wykorzystanie wspólnych zespołów dochodzeniowo-śledczych tworzonych w trybie pilnym	MS wraz z COM, Europolem i Eurojustem	Procedura w toku
Działanie 2: Ochrona gospodarki przed infiltracją przestępczą		
Wniosek w sprawie wsparcia dla antykorupcyjnych działań państw członkowskich oraz ich monitorowania	COM	2011
Utworzenie sieci krajowych punktów kontaktowych dla organów rządowych i regulacyjnych	COM wraz z MS	2011
Działania na rzecz poprawy egzekwowania praw własności intelektualnej i zwalczania sprzedaży podrabianych towarów w Internecie	MS oraz COM	Procedura w toku
Działanie 3: Konfiskata mienia pochodzącego z działalności przestępczej		
Wniosek w sprawie konfiskaty mienia osób trzecich, rozszerzenia kompetencji w zakresie konfiskaty i nakazów konfiskaty bez uprzedniego wyroku skazującego	COM	2011
Utworzenie biur ds. odzyskiwania mienia oraz niezbędne kroki dla zarządzania tym mieniem	MS	2014
Wspólne wskaźniki na potrzeby oceny działalności biur ds. odzyskiwania mienia oraz wytyczne w zakresie zapobiegania odzyskiwaniu skonfiskowanego mienia przez grupy przestępcze	COM	2013

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
CEL 2: Zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów		
Działanie 1: Wzmocnienie pozycji społeczeństwa w zapobieganiu radykalizacji postaw i werbowaniu terrorystów		
Utworzenie unijnej sieci na rzecz uświadamiania na temat radykalizacji wraz z forum internetowym i serią ogólnoeuropejskich konferencji. Wsparcie dla społeczeństwa obywatelskiego w celu ujawniania, tłumaczenia i obalania brutalnej propagandy ekstremistycznej	COM wraz z Komitetem Regionów	2011
Konferencja ministerialna na temat zapobiegania radykalizacji i werbowaniu	COM	2012
Podręcznik na temat zapobiegania radykalizacji, rozbijania kanałów werbunku oraz działania na rzecz rehabilitacji i kreowania postaw negatywnych wobec terroryzmu	COM	2013-14
Działanie 2: Odcięcie terrorystów od ich źródeł finansowania i materiałów oraz śledzenie dokonywanych przez nich transakcji		
Struktury dla zamrażania aktywów terrorystów	COM	2011
Wdrażanie planu działania na rzecz zapobiegania dostępowi do materiałów wybuchowych i substancji chemicznych, biologicznych, radiologicznych i jądrowych	MS	Procedura w toku
Polityka UE w sprawie wydobywania i analizy danych z komunikatów finansowych	COM	2011

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
Działanie 3: Ochrona transportu		
Komunikat w sprawie polityki bezpieczeństwa transportu	COM	2011

CEL 3: Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni		
Działanie 1: Budowa zdolności w zakresie egzekwowania prawa i sądownictwa		
Utworzenie unijnego centrum ds. walki z cyberprzestępczością	Przedmiot studium wykonalności, które COM ukończy w 2011 r.	2013
Rozwój potencjału dochodzeniowo-śledczego i ścigania przestępstw w dziedzinie cyberprzestępczości	MS wraz z CEPOL, Europolem i Eurojustem	2013
Działanie 2: Współpraca z przemysłem w celu wzmacniania pozycji obywateli i ich ochrony		
Stworzenie mechanizmów dla zgłaszania zawiadomień o popełnieniu cyberprzestępstwa i wyposażenie obywateli w informacje na temat bezpieczeństwa cybernetycznego i cyberprzestępczości	MS, COM, Europol, ENISA oraz sektor prywatny	Procedura w toku
Wytyczne dotyczące współpracy w zwalczaniu nielegalnych treści w Internecie	COM wraz z MS i sektorem prywatnym	2011
Działanie 3: Poprawa zdolności reagowania na ataki cybernetyczne		

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
Utworzenie sieci zespołów ds. reagowania kryzysowego w dziedzinie informatycznej w każdym państwie członkowskim oraz jednego takiego zespołu dla instytucji UE, jak również opracowanie krajowych planów awaryjnych i przeprowadzanie ćwiczeń w zakresie reagowania na zagrożenia i odzyskiwania danych	MS i instytucje UE wraz z ENISA	2012
Utworzenie europejskiego systemu ostrzegania i wymiany informacji (EISAS)	MS wraz z COM i ENISA	2013
CEL 4: Poprawa bezpieczeństwa poprzez zarządzanie granicami		
Działanie 1: Wykorzystanie pełnego potencjału EUROSUR		
Wniosek w sprawie ustanowienia EUROSUR	COM	2011
Projekt pilotażowy na południowych i południowo-zachodnich granicach UE	COM, Frontex, Europol, MAOC-N oraz CeCLAD-M	2011
Działanie 2: Zwiększenie wkładu Frontexu w zwalczanie przestępczości na granicach zewnętrznych		
Wspólne sprawozdania na temat handlu ludźmi, przemytu ludzi i przemytu nielegalnych towarów jako podstawa do wspólnych operacji	COM wraz z Frontexem i Europolem	2011
Działanie 3: Wspólne zarządzanie ryzykiem w odniesieniu do przepływu towarów przez zewnętrzne granice UE		
Inicjatywy na rzecz poprawy zdolności w zakresie określania ryzyka i jego analizy	COM	2011

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
Działanie 4: Poprawa współpracy między organami krajowymi		
Opracowanie krajowych analiz wspólnego ryzyka, obejmujących policję, straż graniczną i organy celne w celu identyfikowania newralgicznych punktów na granicach zewnętrznych	MS	2011
Propozycje dotyczące poprawy koordynacji kontroli granicznych przeprowadzanych przez różne organy	COM	2012
Opracowanie minimalnych norm i najlepszych praktyk dla współpracy między różnymi organami	COM, Europol, Frontex, EASO	2014
CEL 5: Zwiększenie odporności Europy na kryzysy i katastrofy		
Działanie 1: Pełne zastosowanie klauzuli solidarności		
Wniosek dotyczący wdrożenia klauzuli solidarności	COM/HR	2011
Działanie 2: Podejście do oceny zagrożenia i ryzyka przy uwzględnieniu wszystkich rodzajów zagrożenia		
Wytyczne dotyczące oceny ryzyka i jego mapowania w ramach zarządzania w przypadku klęsk i katastrof	COM wraz z MS	2010
Krajowe strategie zarządzania ryzykiem	MS	2011-12
Ponadsektorowy przegląd możliwych przyszłych ryzyk naturalnych i tych wywoływanych przez człowieka	COM	2012
Wniosek dotyczący zagrożeń w zakresie zdrowia	COM	2011

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
Regularne przeglądy aktualnych zagrożeń	COM wraz z MS i CTC	2013
Opracowanie spójnej polityki zarządzania ryzykiem	COM wraz z MS	2014
Działanie 3: Połączenie w sieć różnych ośrodków służących obserwacji położenia		
Wzmocnienie powiązań pomiędzy sektorowymi systemami wczesnego ostrzegania i mechanizmami współpracy kryzysowej	COM	2012
Wniosek w sprawie spójnych ogólnych ram dla ochrony informacji niejawnych	COM	2011
Działanie 4: Utworzenie europejskiego potencjału reagowania w przypadku klęsk i katastrof		
Wniosek w sprawie stworzenia europejskiego potencjału reagowania kryzysowego	COM	2011