



KOMISJA EUROPEJSKA

Bruksela, dnia 25.11.2011
KOM(2011) 790 wersja ostateczna

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

**Pierwsze sprawozdanie roczne w sprawie wykonania strategii bezpieczeństwa
wewnętrznego UE**

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Pierwsze sprawozdanie roczne w sprawie wykonania strategii bezpieczeństwa wewnętrznego UE

I. Wprowadzenie

W lipcu bieżącego roku prawicowy ekstremista przeprowadził w Norwegii krwawy atak terrorystyczny. W sierpniu organy publiczne Zjednoczonego Królestwa zajęły rekordową ilość 1,2 milionów ton kokainy. W całej UE ataki cybernetyczne powodują coraz większe spustoszenia w prywatnych i publicznych systemach komputerowych. Wydarzenia te dobitnie przypominają o tym, jak duże znaczenie mają działania służące przeciwstawianiu się zagrożeniom dla bezpieczeństwa wewnętrznego.

W „Strategii bezpieczeństwa wewnętrznego UE w działaniu”¹, przyjętej w listopadzie 2010 r., nakreślono priorytety, na których UE powinna skoncentrować się w nadchodzących czterech latach, a należą do nich: 1) rozbijanie międzynarodowych siatek przestępczych, 2) zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów, 3) podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni, 4) poprawa bezpieczeństwa poprzez zarządzanie granicami oraz 5) zwiększenie odporności Europy na kryzysy i katastrofy.

W marę jak pojawiają się nowe zagrożenia dla bezpieczeństwa, a istniejące ewoluują, UE musi być gotowa do działania. Konieczne są regularne oceny zagrożeń i ryzyka przeprowadzane przez agencje UE takie jak Europol, Eurojust, Frontex oraz Centrum Sytuacyjne Unii Europejskiej (SitCen).

W najnowszym sprawozdaniu Europolu² zidentyfikowano trzy nowe zagrożenia, wzbudzające szczególne zaniepokojenie.

Po pierwsze, kwestie dotyczące szybkich zmian zachodzących w **technologii internetowej**. Internet stanowi obecnie integralny i nieodłączny element codziennego życia obywateli UE, staje się też jednak istotnym czynnikiem ułatwiającym działalność przestępczą i nośnikiem propagandy terrorystycznej. Rosnące uzależnienie od technologii internetowej czyni nasze społeczeństwo coraz bardziej narażonym na poważne włamania do systemów komputerowych, które mogą być skierowane przeciwko administracjom, przemysłowym systemom sterowania lub bankom.

Po drugie, potencjalne implikacje **trwającego kryzysu gospodarczego**. Rosnące ograniczenia finansowe mogą doprowadzić do zmniejszenia środków dostępnych dla organów publicznych na cele walki w zagrożeniami dla bezpieczeństwa wewnętrznego. Nie istnieje oczywiste i natychmiastowe rozwiązanie – jednak wszyscy powinniśmy mieć świadomość ograniczeń i ich konsekwencji.

¹ Komunikat Komisji: Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy – COM(2010) 673/3 (dalej zwany „Strategią bezpieczeństwa wewnętrznego w działaniu”).

² Zob. Europol: Organised Crime Threat Assessment (OCTA) 2011.

Po trzecie, wpływ **zewnętrznego wymiaru bezpieczeństwa** na UE. Bezpieczeństwo wewnętrzne UE jest ściśle związane z poziomem bezpieczeństwa w jej otoczeniu, co pokazały niedawne wydarzenia w świecie arabskim. Te obiecujące wydarzenia, wnoszące demokrację i dobrobyt w regionie, spowodowały również znaczące przepływy ludności, zwiększając presję na zdolności państw sąsiadujących w zakresie zarządzania granicami, w tym granicą zewnętrzną UE. Podobnie trwające wysiedlenia ludności oraz luki w zarządzaniu mogą tworzyć warunki dla nasilonej działalności kryminalnej i terrorystycznej w regionie Sahelu. Na południowy wschód od UE państwa Bałkanów Zachodnich w dalszym ciągu są źródłem niepokoju ze względu na utrzymującą się działalność międzynarodowej przestępczości zorganizowanej, jak nielegalny handel narkotykami, ludźmi i podrabianymi towarami.

Konieczność koordynacji na szczeblu UE, aby sprostać tym wyzwaniom, nigdy dotąd nie była większa. W nadchodzących latach konieczne będzie wdrożenie zidentyfikowanych działań. To jednak nie wystarczy. Cele strategiczne będą musiały się przełożyć na konkretne plany i działania. W tym względzie Komisja z zadowoleniem przyjmuje metodykę unijnego cyklu politycznego „Harmonia”, w ramach którego priorytety polityczne i oceny zagrożeń zostaną przełożone na operacyjne plany działania, zwłaszcza w obszarach poważnej przestępczości międzynarodowej i zorganizowanej, cyberprzestępczości i zarządzania granicami, poprzez realizację ośmiu priorytetów uzgodnionych w Radzie.³

Kontynuując realizację strategii bezpieczeństwa wewnętrznego UE w działaniu, Komisja będzie w dalszym ciągu zapewniać pełne poszanowanie rządów prawa i Europejskiej Karty Praw Podstawowych, w tym prawa jednostek do prywatności.

W poniższym sprawozdaniu przedstawiono ocenę realizacji strategii bezpieczeństwa wewnętrznego w działaniu w 2011 r. Opisano w nim stan unijnej polityki bezpieczeństwa w zakresie każdego z pięciu celów strategii bezpieczeństwa wewnętrznego⁴ i przedstawiono perspektywy działań w 2012 r. W załączniku przedstawiono szczegółową ocenę najważniejszych środków wdrożonych w 2011 r.

II. Stan bezpieczeństwa wewnętrznego UE

1. Przestępczość zorganizowana/międzynarodowe siatki przestępcze

Wyłania się nowy krajobraz przestępczości, który charakteryzuje się coraz bardziej mobilnymi i elastycznymi grupami funkcjonującymi w wielu systemach prawnych i gałęziach przestępczości, przy pomocy zwłaszcza szeroko rozpowszechnionego wykorzystywania internetu do nielegalnych celów. Grupy o największych zasobach zdywersyfikowały swoje interesy w zakresie działalności przestępczej, zwiększając w ten sposób swoją odporność w czasach oszczędności gospodarczych i wzmacniając swoją zdolność do identyfikowania i wykorzystywania nowych nielegalnych rynków. Coraz większe zainteresowanie zorganizowanych grup przestępczych przyciągają działania wiążące się z niskim poziomem

³ Zob. konkluzje Rady w sprawie określenia priorytetów UE w zwalczaniu przestępczości zorganizowanej w latach 2011–2013; dokumenty: 11050/11, JAI 396 COSI 46 ENFOPOL 184 CRIMORG 81 ENFOCUSTOM 52 PESC 718 RELEX 603. Zob. również załącznik.

⁴ Sprawozdanie zostało opracowane przez Europol przy współpracy Eurojustu, agencji Frontex, Komisji/DG ECHO, m.in. w oparciu o dokumenty strategiczne – Europol’s Organised Crime Threat Assessment (OCTA) 2011, Terrorism Situation and Trend Report (TE-SAT) 2011, Frontex’ Annual Risk Analysis (ARA) 2011 oraz Western Balkans Annual Risk Analysis (WB ARA) 2011 – a także na sprawach prowadzonych przez Eurojust, odzwierciedlonych w sprawozdaniu rocznym za 2010 r.

ryzyka, takie jak oszustwa w zakresie jednostek emisji, kart płatniczych i podrabianie towarów.

Chociaż cele terrorystów i zorganizowanych grup przestępczych są różne, powiązania między działalnością terrorystyczną a przestępczością zorganizowaną wydają się być coraz silniejsze. Przestępczość jest powszechnie wykorzystywana w celu finansowania działań terrorystycznych⁵. Grupy terrorystyczne mogą być bezpośrednio zaangażowane w przestępczość zorganizowaną lub powiązane z indywidualnymi przestępcami lub grupami przestępczymi, w dziedzinach takich jak handel bronią i narkotykami, handel ludźmi, oszustwa finansowe, pranie pieniędzy i wymuszenia.

Współpraca międzynarodowa między organami ma zasadnicze znaczenie dla sprostania wyzwaniom w zakresie bezpieczeństwa wewnętrznego UE. Jednak dostępne instrumenty wymiany informacji, zwłaszcza inicjatywa szwedzka⁶ i decyzje z Prüm⁷ wciąż nie zostały w pełni wdrożone w państwach członkowskich. Potrzebna jest jeszcze większa spójność i konsolidacja międzynarodowej wymiany informacji na temat egzekwowania prawa.

Obywatele europejscy potrzebują pewności, że skutecznemu rozbijaniu działalności siatek przestępczych towarzyszy koordynacja skutecznego i sprawiedliwego ścigania. Jednakże różne instrumenty współpracy sądowej i organów ścigania czekają jeszcze na ratyfikację i wdrożenie przez wszystkie państwa członkowskie⁸. Ponadto różne wymagania państw członkowskich w odniesieniu do międzynarodowych rewizji lub zajęć mogą utrudniać koordynację pilnych działań w różnych systemach prawnych. Europejski nakaz dochodzeniowy wzmocniłby zasadę wzajemnego uznawania i byłby odpowiedzią na bieżące trudności w uzyskiwaniu informacji i dowodów w sprawach transgranicznych.

Całkowita wartość środków zamrożonych i skonfiskowanych w UE utrzymuje się na bardzo niskim poziomie w porównaniu z szacunkową wartością majątku organizacji przestępczych. Skuteczniejsze wykrywanie i zajmowanie środków pochodzących z działalności przestępczej wymaga intensywniejszych starań. Przestępczość zorganizowana poszukuje możliwości dalszego inwestowania środków w legalne działania, co oznacza potrzebę bardziej rygorystycznych przepisów służących zwalczaniu prania pieniędzy oraz większej koncentracji działalności operacyjnej na sposobach, w jaki przestępcy przenikają do legalnej gospodarki.

Aby wzmocnić unijne narzędzia służące do walki z przestępczością zorganizowaną, w 2011 r. Komisja przyjęła między innymi pakiet legislacyjny dotyczący walki z korupcją, a także przedstawiła wniosek prawodawstwa UE w sprawie gromadzenia danych dotyczących przelotu pasażera na lotach do lub z terytorium UE.

⁵ Zob. Europol: EU Terrorism Situation and Trend Report (TE-SAT) 2011.

⁶ Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r.

⁷ Decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW (decyzje z Prüm).

⁸ Takie jak europejska konwencja o przekazywaniu ścigania w sprawach karnych z 1972 r. oraz Konwencja o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej z 2000 r.

Perspektywy na 2012 r.

Komisja:

- **przyjmie pakiet legislacyjny dotyczący konfiskaty i odzyskania mienia pochodzącego z działalności przestępczej;**
- **przedstawi wniosek dotyczący reformy Europolu i CEPOLu oraz europejskiego systemu szkoleniowego;**
- **przedstawi wniosek dotyczący reformy Eurojustu;**
- **będzie dążyć do zawarcia dwóch nowych porozumień PNR ze Stanami Zjednoczonymi i Kanadą;**
- **będzie działać na rzecz przyjęcia jej wniosku dotyczącego dyrektywy w sprawie gromadzenia danych dotyczących przelotu pasażera;**
- **przedstawi komunikat na temat europejskiego modelu wymiany informacji;**
- **opracuje strategię w zakresie dochodzeń finansowych;**
- **przedstawi wniosek dotyczący zmienionej dyrektywy w sprawie przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu; oraz**
- **opublikuje pięcioletnią strategię dotyczącą handlu ludźmi.**

Państwa członkowskie zachęca się do:

- **realizacji działań przewidzianych w unijnym cyklu politycznym;**
- **zintensyfikowania starań zmierzających do rozwinięcia podejścia administracyjnego angażującego wszystkie organy sektora publicznego, a nie tylko organy ścigania, w celu ochrony gospodarki przed przestępczością i korupcją;**
- **dokonywania postępów w tworzeniu skutecznych biur ds. odzyskiwania mienia oraz w ułatwianiu wymiany informacji i najlepszych praktyk;**
- **ratyfikacji i wdrożenia istniejących instrumentów służących współpracy sądowej i wymiaru sprawiedliwości oraz wymianie informacji, w szczególności inicjatywy szwedzkiej, dyrektywy o zatrzymywaniu danych i decyzji z Prüm, jak również konwencji o przeniesieniu postępowania oraz wzajemnej pomocy w sprawach karnych; oraz**
- **niezwłocznej transpozycji dyrektywy dotyczącej handlu ludźmi.**

2. Terroryzm i radykalizacja postaw

Dziesięć lat po wydarzeniach z 11 września statystyki dotyczące osób podejrzanych o terroryzm wskazują, że terroryzm islamski w dalszym ciągu stanowi przeważające zagrożenie dla UE. Niemniej jednak tragiczne wydarzenia, które miały miejsce w lipcu w Norwegii przypomniły nam, że zagrożenie, jakie niesie ze sobą terroryzm nie ogranicza się do jednego zestawu politycznych czy religijnych ideologii lub motywacji: Sieć pierwszej reakcji, utworzona na fali ataków terrorystycznych w Londynie w 2005 r. została po raz pierwszy aktywowana po ataku w Norwegii i okazała się przydatna.

Rodzimy terroryzm i radykalizacja postaw obywateli UE jest rosnącym źródłem niepokoju. UE musi wyprzedzać zmiany zarówno pod względem procesu radykalizacji postaw, jak i wykorzystywanej technologii. Uruchomiona we wrześniu 2011 r. unijna sieć upowszechniania wiedzy o radykalizacji postaw, ma na celu ułatwianie dzielenia się wiedzą, podnoszenie świadomości oraz wyszukiwanie nowych, twórczych rozwiązań służących do walki w brutalnym ekstremizmem. Komisja zapewni przyjęcie spójnego podejścia z Europejską Służbą Działań Zewnętrznych (EEAS) i koordynatorem UE ds. zwalczania terroryzmu wobec przeciwdziałania brutalnemu ekstremizmowi zarówno wewnątrz UE, jak i na zewnątrz.

Ryzyka radykalizacji postaw jednostek nie da się całkowicie wyeliminować. Dlatego inicjatywy na rzecz uniemożliwiania terrorystom dostępu do finansowania i materiałów oraz służące zwiększeniu bezpieczeństwa transportu będą miały zasadnicze znaczenie w walce z terroryzmem. W 2010 r. Komisja przedstawiła unijny plan działania mający na celu zwiększenie bezpieczeństwa ładunków lotniczych, zawierający nowe reguły i definicję kryteriów identyfikacji ładunku wysokiego ryzyka, a obecnie weszła już w końcową fazę rozwoju unijnej oceny ryzyka dla bezpieczeństwa lotniczego. Ponadto udoskonalona wymiana informacji z Europolem i Eurojustem ułatwiłaby zarówno zapobieganie działalności terrorystycznej, jak i późniejsze jej ściganie.

Perspektywy na 2012 r.

Komisja:

- **zorganizuje konferencję na wysokim szczeblu na temat zwalczania brutalnego ekstremizmu przy wsparciu unijnej sieci upowszechniania wiedzy o radykalizacji postaw;**
- **przygotuje zestaw wniosków odnoszących się do kwestii wykorzystywania internetu przez terrorystów, przeanalizowawszy możliwości przeciwdziałania radykalizacji postaw w internecie;**
- **przedstawi wniosek dotyczący instrumentu legislacyjnego w sprawie zamrażania środków w celu zwalczania terroryzmu i powiązanych działań;**
- **dokona przeglądu dyrektywy w sprawie ustanowienia ochrony europejskiej infrastruktury krytycznej;**
- **przedstawi sprawozdanie śródkresowe na temat realizacji planu działania UE w obszarze CBRJ oraz przegląd planu działania UE w zakresie materiałów wybuchowych; oraz**

- **zaproponuje możliwości utworzenia unijnego systemu śledzenia środków finansowych w oparciu o dyskusje z Radą i Parlamentem Europejskim; oraz**
- **zaproponuje możliwości dalszego zwiększenia bezpieczeństwa transportu, skupiając się przede wszystkim na kwestiach dotyczących transportu lądowego.**

Państwa członkowskie zachęca się do:

- **realizacji planu działania dotyczącego bezpieczeństwa ładunków lotniczych; oraz**
- **zintensyfikowania starań na rzecz przeciwdziałania brutalnemu ekstremizmowi.**

3. Cyberprzestępczość i bezpieczeństwo cybernetyczne

Unia Europejska jest zasadniczym celem cyberprzestępczości ze względu na rozbudowaną infrastrukturę internetową, powszechne wykorzystanie internetu oraz gospodarkę i systemy płatnicze coraz silniej związane z internetem. Ze względu na tempo rozwoju technologicznego oraz jego zaawansowanie cyberprzestępczość nieprzerwanie się rozwija. Nowe trendy technologiczne, jak rozwój przetwarzania w chmurze i coraz powszechniejsze korzystanie z urządzeń przenośnych, powodują dodatkowe zagrożenia dla użytkowników i zwiększają wyzwania dla organów ścigania⁹. Powszechne korzystanie z technologii internetowej w UE przyczyniło się również do bezprecedensowej ekspansji na rynkach materiałów o treściach związanych z wykorzystywaniem dzieci i kradzieży własności intelektualnej.

internet nie zna granic, ale jurysdykcja w ściganiu cyberprzestępstw wciąż zatrzymuje się na granicach państw. Państwa członkowskie muszą połączyć wysiłki na poziomie UE, aby przygotować wspólną reakcję. Wiązałoby się to z intensywniejszym wykorzystaniem istniejącego potencjału unijnych agencji. Do zwiększenia zdolności UE do walki z cyberprzestępczością przyczyni się także współpraca z partnerami międzynarodowymi.

W 2011 r. dokonano pewnych osiągnięć w kierunku przygotowania gruntu pod utworzenie europejskiego centrum ds. walki z cyberprzestępczością, jak również wspierania państw członkowskich w tworzeniu krajowych/rządowych zespołów ds. reagowania kryzysowego w dziedzinie informatycznej. Grupa robocza UE/USA w dziedzinie bezpieczeństwa cybernetycznego i cyberprzestępczości przynosi rezultaty, począwszy od współpracy w zakresie zwalczania dziecięcej pornografii po wspólne ćwiczenia w przeciwdziałaniu atakom cybernetycznym.

⁹ Zob. Europol: Threat Assessment on internet Facilitated Organised Crime (iOCTA) 2011 r.

Perspektywy na 2012 r.

Komisja:

- opracuje nadrzędną europejską strategię bezpieczeństwa internetowego;
- dokona wszelkich uzgodnień dotyczących konfiguracji europejskiego centrum ds. walki z cyberprzestępczością do 2013 r.; oraz
- będzie opierać się na pracy wykonanej przez grupę roboczą UE/USA w dziedzinie bezpieczeństwa cybernetycznego i cyberprzestępczości i zainicjuje współpracę z innymi partnerami międzynarodowymi.

Państwa członkowskie zachęca się do:

- realizacji działań przewidzianych w unijnym cyklu politycznym;
- kontynuacji działań na rzecz podnoszenia krajowej świadomości w zakresie cyberprzestępczości i rozwijania zdolności szkoleniowych oraz tworzenia centrów doskonałości;
- ratyfikacji Konwencji Rady Europy o cyberprzestępczości¹⁰;
- utworzenia krajowych/rządowych zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (CERT) oraz sprawnie działającej sieci;
- a także do doskonalenia systemów sprawozdawczości na temat cyberprzestępczości.

4. Zarządzanie granicami

W 2011 r. państwa członkowskie i Frontex musiały nasilić starania w zakresie przeciwdziałania rosnącej presji na zewnętrzne granice UE. Od czasu rozpoczęcia „Operacji Hera” w 2006 r. Frontex odniósł sukces zamykając trasę nielegalnej migracji z Afryki Zachodniej na Wyspy Kanaryjskie. Na wschodniej granicy UE utrzymuje się przymęt na szeroką skalę. Komisja przedstawiła jednak w tym roku szereg działań, które należy podjąć, aby rozwiązać ten problem¹¹. Śródziemnomorska granica morska oraz granica lądowa z Turcją są obecnie najważniejszymi punktami nielegalnego przekraczania granicy i sytuacja ta prawdopodobnie się utrzyma.

W następstwie niedawnych wydarzeń w Afryce Północnej ponad 50 000 migrantów przedostało się na terytorium UE przez śródziemnomorską granicę morską, często przy pomocy siatek przestępczych. Uruchomienie „wspólnej operacji Hermes” Frontexu w lutym 2011 r. odegrało zasadniczą rolę w patrolowaniu tego szlaku. Również zespół szybkiej interwencji na granicy (RABIT) agencji Frontex, który po raz pierwszy w historii udzielił wsparcia w zakresie zarządzania granicami na granicy lądowej między Grecją i Turcją, w

¹⁰ Austria, Belgia, Republika Czeska, Grecja, Irlandia, Luksemburg, Malta, Polska i Szwecja nie ratyfikowały jeszcze konwencji.

¹¹ http://ec.europa.eu/anti_fraud/documents/Working-paper.pdf

okresie swojego działania przyczynił się do ograniczenia liczby nielegalnych przekroczeń granicy o 75%.

W styczniu 2011 r. Komisja przedstawiła ramy europejskiego systemu nadzoru granic (EUROSUR). FRONTEX we współpracy z sześcioma państwami członkowskimi uruchomił projekt pilotażowy na lądowo-morskiej granicy zewnętrznej. Wywarło to wpływ na wniosek ustawodawczy Komisji w sprawie EUROSUR, który zostanie przedstawiony w grudniu 2011 r., aby system mógł rozpocząć działalność w 2013 r.

Zarządzanie granicami zewnętrznymi musi sprzyjać jednocześnie zwiększaniu bezpieczeństwa, jak i ułatwianiu podróży. W związku z tymi celami w 2011 r. Komisja przedstawiła wnioski dotyczące udoskonalonego systemu oceny i monitorowania Schengen oraz analizę potencjalnego wprowadzenia systemów wjazdu/wyjazdu oraz rejestracji podróżnych, do czego wzywała Rada.

Perspektywy na 2012 r.

Komisja:

- **przedstawi wnioski na podstawie wyników dyskusji na temat komunikatu w sprawie inteligentnych granic (system wjazdu/wyjazdu i rejestracji podróżnych); oraz**
- **przedstawi sugestie dotyczące sposobu udoskonalenia koordynacji kontroli granicznych przeprowadzanych przez różne organy krajowe (policję, straż graniczną i służby celne).**

Państwa członkowskie zachęca się do:

- **realizacji działań przewidzianych w unijnym cyklu politycznym;**
- **kontynuacji starań na rzecz utworzenia EUROSUR; oraz**
- **aktywnego udziału w dialogach na temat migracji, mobilności i bezpieczeństwa z nowymi rządami państw Afryki Północnej i Bliskiego Wschodu.**

5. Zarządzanie kryzysowe i na wypadek katastrof

W ciągu ostatnich lat obywatele europejscy doświadczyli różnych klęsk, zarówno naturalnych, jak i spowodowanych działalnością człowieka. Utrzymuje się zagrożenie wrogimi atakami, jak ataki terrorystyczne czy cybernetyczne lub wrogie bądź przypadkowe uwolnienie czynników chorobotwórczych i patogenów. Trzęsienie ziemi w Aquili we Włoszech, kryzys spowodowany chmurą popiołu wulkanicznego na skutek erupcji wulkanu w Islandii oraz lipcowy atak terrorystyczny w Norwegii zwiększają potrzebę wzmocnienia zdolności UE w zakresie zarządzania kryzysowego. Ponadto wypadek w elektrowni Fukushima uwidoczniał nie tylko możliwość wystąpienia łańcucha zdarzeń przyczynowo-skutkowych – od trzęsienia ziemi przez tsunami po kryzys nuklearny – lecz także globalne skutki tych zdarzeń, na przykład dla transportu międzynarodowego, ceł i bezpieczeństwa żywności, które wymagają złożonych rozwiązań w zakresie zarządzania ryzykiem.

Złożony charakter i zakres tych wyzwań powoduje potrzebę kompleksowego podejścia do oceny ryzyka, opracowywania prognoz, profilaktyki, przygotowania się do klęsk i łagodzenia ich skutków. Wymaga to połączenia różnych aspektów polityki, instrumentów i usług dostępnych UE i państwom członkowskim.

Za pośrednictwem Europolu, agencji Frontex, Centrum Sytuacyjnego Unii Europejskiej (SitCen) i Centrum Monitorowania oraz Informacji przy Komisji Europejskiej UE jest w stanie opierać się na potencjale i wiedzy fachowej w zakresie gromadzenia informacji, analizy, oceny zagrożeń i reagowania kryzysowego w różnych dziedzinach bezpieczeństwa wewnętrznego. Jednak jednym z najważniejszych wyzwań na nadchodzące lata pozostaje stopniowe dążenie w kierunku spójnej polityki zarządzania ryzykiem łączącej ocenę zagrożenia i ryzyka z opracowywaniem i realizowaniem polityki. Poczyniono ponad 2011 wstępnych kroków w tym kierunku.

Perspektywy na 2012 r.

Komisja:

- przyczyni się do dalszego rozwoju unijnej polityki oceny zagrożenia i ryzyka, a także przygotuje przegląd najważniejszych zagrożeń naturalnych i spowodowanych działalnością człowieka, przed jakimi UE może stanąć w przyszłości;
- rozwinie bardziej swoje zdolności w zakresie oceny strategicznej, w szczególności poprzez połączenie istniejącej wiedzy fachowej różnych podmiotów (Europol, Frontex i SitCen) w dziedzinie bezpieczeństwa wewnętrznego; oraz
- przedstawi wraz z wysoką przedstawiciel do spraw zagranicznych i polityki bezpieczeństwa wspólny wniosek dotyczący wprowadzenia klauzuli solidarności.

Państwa członkowskie zachęca się do:

- opracowywania regularnych ocen zagrożenia i ryzyka; oraz
- wspierania wysiłków zmierzających do zwiększenia europejskiego potencjału w zakresie reagowania w przypadku klęsk.

III. Wniosek

W niniejszym sprawozdaniu na temat bezpieczeństwa wewnętrznego UE podkreślono pewne kwestie, które powinny zostać poddane dalszej analizie przez Parlament Europejski, państwa członkowskie, Komisję i społeczeństwo ogółem.

Zagrożenia opisane w strategii bezpieczeństwa wewnętrznego w działaniu z listopada 2010 r. nie straciły na znaczeniu w 2011 r. i powinny w dalszym ciągu stanowić centrum działań UE w zakresie bezpieczeństwa wewnętrznego.

W walce z przestępczością zorganizowaną osiągnięto znaczące postępy, w szczególności w związku z wnioskiem dotyczącym unijnego prawodawstwa w zakresie gromadzenia danych dotyczących przelotu pasażera na lotach do lub z terytorium UE oraz pakietem w sprawie walki z korupcją. Potrzebne są dalsze postępy w zakresie współpracy sądowej i wymiaru sprawiedliwości, a także rozwoju podejścia administracyjnego w walce przeciwko poważnej przestępczości.

Jeżeli chodzi o **terroryzm i radykalizację postaw**, osiągnięcia obejmują w szczególności ustanowienie sieci upowszechniania wiedzy o radykalizacji postaw. Przyjęcie komunikatu na temat unijnego systemu śledzenia środków finansowych również stanowi istotny krok naprzód. Konieczne są jednak intensywniejsze działania, w szczególności w odniesieniu do ram środków administracyjnych w zakresie zamrażania mienia terrorystów i zwiększenia bezpieczeństwa transportu lądowego.

Dobrze rozwijają się działania służące walce z **cyberprzestępczością**. Poczyniono postępy w kierunku utworzenia europejskiego centrum ds. walki z cyberprzestępczością i zespołów ds. reagowania kryzysowego w dziedzinie informatycznej. Kilka państw członkowskich musi podjąć pilne działania w celu ratyfikacji konwencji budapeszteńskiej.

W dziedzinie **zarządzania granicami** utworzenie systemu EUROSUR jest w toku, jednak usprawnienie współpracy między agencjami na szczeblu krajowym wymaga dalszej debaty na temat wniosków dotyczących inteligentnych granic i dalszych działań.

W działaniach związanych z **zarządzaniem kryzysowym** również odnotowano postępy. W 2011 r. podjęto pracę przykładowo w dziedzinie oceny ryzyka. Jeżeli chcemy osiągnąć założony cel, w dziedzinie zarządzania kryzysowego konieczne są jednak dodatkowe starania. Zasadnicze znaczenie ma pełne zaangażowanie państw członkowskich, Komisji i ESDZ oraz współpraca między nimi.

W celu zniwelowania przepaści między bezpieczeństwem wewnętrznym a zewnętrznym przeprowadzono zaawansowane prace. Opracowano kilka inicjatyw mających na celu wspieranie współpracy i koordynacji: obejmuje to praktyczną współpracę w zakresie terroryzmu, przestępczości transgranicznej oraz nielegalnej migracji na Bałkanach Zachodnich, w Rogu Afryki oraz w Sahelu. Ponadto ESDZ i Komisja opracowały wspólny dokument na temat zacieśniania więzi między podmiotami wspólnej polityki bezpieczeństwa i obrony (WPBiO) i wolności, bezpieczeństwa i sprawiedliwości (WSiSW); w tym możliwości współpracy między misjami policyjnymi WPBiO i Europolem.

Sukces każdej strategii zależy od jej zdolności do przynoszenia wymiernych rezultatów. W przypadku strategii bezpieczeństwa wewnętrznego w działaniu rok 2011 był obiecującym początkiem. Pozostają jednak jeszcze trzy lata. Wiele należy zrobić, aby zapewnić bezpieczeństwo obywateli europejskich. Do czasu kolejnego sprawozdania rocznego

konieczne są postępy w zakresie wszystkich priorytetów, w szczególności jednak w walce z poważną i zorganizowaną przestępczością, jak również w walce z rosnącym zagrożeniem cybernetycznym.

Załącznik

Realizacja celów strategii bezpieczeństwa wewnętrznego w 2011 r.

W niniejszym załączniku przedstawiono aktualne informacje na temat realizacji pięciu priorytetów strategii bezpieczeństwa wewnętrznego UE w działaniu wraz z informacjami na temat najważniejszych rezultatów z 2011 r. oraz tabelą ilustrującą stan działań w zakresie środków przewidzianych w ramach każdego z celów.

Od czasu przyjęcia strategii bezpieczeństwa wewnętrznego w działaniu w 2010 r. Rada przyjęła również unijny cykl polityczny „Harmonia” w zakresie przestępczości zorganizowanej 2011–2013. Obejmuje on osiem priorytetów koncentrujących się na działaniach w zakresie poważnej i zorganizowanej przestępczości, cyberprzestępczości i wzmacniania zarządzania granicami¹². Metodyka ta stanowi istotny krok w przekładaniu priorytetów politycznych i strategii bezpieczeństwa wewnętrznego na działania przynoszące konkretne zbiorowe rezultaty dla bezpieczeństwa wewnętrznego.

Cel 1 – rozbijanie międzynarodowych siatek przestępczych

Unijne dane dotyczące przelotu pasażera (dane PNR)

W lutym 2011 r. Komisja przedstawiła wniosek legislacyjny w sprawie gromadzenia danych dotyczących przelotu pasażera na lotach do lub z terytorium UE. Jego celem jest umożliwienie właściwym organom państw członkowskich analizowania danych w celu uniemożliwienia, wykrywania i ścigania przestępstw terrorystycznych i poważnych przestępstw. Wniosek jest obecnie omawiany przez Parlament Europejski i Radę. Wniosek stanowi część szerszej polityki w zakresie danych PNR, która obejmuje zawarcie porozumień PNR z krajami trzecimi. Porozumienia takie umożliwiają wykorzystanie danych PNR pochodzących z UE przez organy ścigania tych państw w tym samym celu. Istniejące

¹² Unijny cykl polityczny „Harmonia” obejmuje osiem następujących priorytetów:

1. zmniejszenie potencjału zorganizowanych grup przestępczych aktywnych w Afryce Zachodniej lub mających tam siedziby, zajmujących się sprowadzaniem do UE kokainy i heroiny lub ich rozprowadzaniem w UE;
2. zmniejszenie roli Bałkanów Zachodnich jako kluczowej strefy tranzytu i składowania nielegalnych towarów przeznaczonych na rynki Europy oraz centrum logistycznego zorganizowanych grup przestępczych, w tym zorganizowanych grup przestępczych złożonych z osób mówiących po albańsku;
3. zmniejszenie zdolności zorganizowanych grup przestępczych w zakresie ułatwiania nielegalnej migracji do UE, w szczególności poprzez Europę Południową, Południowo-Wschodnią i Wschodnią, a w szczególności przez granicę grecko-turecką oraz w kryzysowych obszarach w basenie Morza Śródziemnego, w pobliżu Afryki Północnej;
4. ograniczenie produkcji i dystrybucji w UE narkotyków syntetycznych, w tym nowych substancji psychoaktywnych;
5. dezorganizacja dostaw, w szczególności kontenerowych, nielegalnych towarów do UE, w tym kokainy, heroiny, konopi indyjskich, towarów podróbionych i papierosów;
6. zwalczanie wszystkich form handlu ludźmi i przemytu ludzi, dzięki skoncentrowaniu działań na zorganizowanych grupach przestępczych prowadzących takie działania w szczególności w centrach przestępczości na południu, południowym zachodzie i południowym wschodzie UE;
7. ograniczenie ogólnych zdolności mobilnych zorganizowanych grup przestępczych do angażowania się w działalność przestępczą;
8. nasilenie zwalczania cyberprzestępczości i wykorzystania internetu do celów przestępczych przez zorganizowane grupy przestępcze.

porozumienia z Kanadą i USA są aktualnie przedmiotem powtórnych rokowań, natomiast we wrześniu 2011 r. podpisane zostało nowe porozumienie z Australią.

W rocznym programie prac¹³ programu „Zapobieganie i walka z przestępczością” na 2012 r. Komisja uwzględniła 25 mln EUR w postaci możliwości finansowania na rzecz tworzenia biur ds. PNR w państwach członkowskich.

Wspólne zespoły dochodzeniowo-śledcze

Aby wspierać tworzenie wspólnych zespołów dochodzeniowo-śledczych – zwłaszcza z krótkim wyprzedzeniem – oraz aby wywrzeć pozytywne praktyczne skutki na walkę z przestępczością transgraniczną, Komisja przydzieliła drugą transzę środków o wartości 2,1 mln EUR na rzecz projektu wspólnych zespołów dochodzeniowo-śledczych Eurojustu „Wspieranie szerszego wykorzystania wspólnych zespołów dochodzeniowo-śledczych”. Projekt wspiera tworzenie nowych wspólnych zespołów dochodzeniowo-śledczych oraz istniejące już zespoły, polepszając ich dostęp do pomocy finansowej w nadchodzących latach. W ciągu pierwszego roku istnienia bieżącego projektu Eurojustu udzielono już wsparcia 33 wspólnym zespołom dochodzeniowo-śledczym, badającym różne przestępstwa, takie jak handel narkotykami, handel ludźmi, nielegalna migracja, przestępczość samochodowa, cyberprzestępczość i przestępstwa finansowe. Europol przyczynił się również do utworzenia i funkcjonowania wspólnych zespołów dochodzeniowo-śledczych dzięki swojej szybkiej i bezpiecznej sieci komunikacji i wymiany informacji, wsparciu logistycznemu i kryminalistycznemu oraz potencjałowi analitycznemu.

Przykład 1:

Eurojust wspierał między innymi odnoszący sukcesy wspólny zespół dochodzeniowo-śledczy utworzony przez Niemcy i Rumunię, który badał działalność zorganizowanej grupy przestępczej zaangażowanej w handel ludźmi. W wyniku tego dochodzenia 50 sprawcom postawiono zarzuty handlu ludźmi i powiązanych przestępstw, 6 oskarżonych otrzymało już wyroki skazujące, przesłuchano 148 świadków i zajęto 860 000 EUR (w gotówce i mieniu innego rodzaju). W ramach projektu finansowania JIT Eurojust udzielił pomocy w sfinansowaniu kosztów podróży i zakwaterowania członków zespołów dochodzeniowo-śledczych, co umożliwiło bezpośrednią komunikację i realizację wspomnianych wyżej wspólnych działań dochodzeniowych. Wsparcia finansowego udzielono także na cele tłumaczenia materiałów dochodzeniowych.

Przykład 2:

Wielostronny zespół dochodzeniowo-śledczy (JIT) koordynowany przez Eurojust odegrał zasadniczą rolę w sukcesie dochodzenia i ścigania przemytu kokainy na dużą skalę z Ameryki Południowej do Europy. Porozumienie JIT zostało podpisane na początkowy okres sześciu miesięcy, a następnie kilkakrotnie przedłużone w celu umożliwienia nieprzerwanej pracy przez ponad dwa lata. W ramach zespołu dochodzeniowo-śledczego organy śledcze i sądownicze spotykały się regularnie, aby podejmować decyzje na temat wspólnych strategii, i

¹³ C (2011) 6306 wersja ostateczna; przyjęty w dniu 19 września 2011 r.

wymieniały się informacjami i dowodami bez opóźnień związanych z tradycyjnymi wnioskami o wzajemną pomoc prawną. Prokuratorzy i organy ścigania z państwa X byli obecni w czasie przesłuchań podejrzanych w państwie Y. Wyznaczenie liderów zespołu JIT z prawem przewodniczenia całemu zespołowi podczas prowadzenia działań we własnym państwie ułatwiło szybkie wykonanie środków egzekwowania prawa i współpracy sądowej w różnych jurysdykcjach. Eurojust koordynował prace zespołu dochodzeniowo-śledczego na spotkaniach w Hadze z aktywnym udziałem i wkładem analitycznym Europolu. Finansowanie zespołów JIT przez Eurojust zostało wykorzystane w odniesieniu do kosztów tłumaczeń ustnych, tłumaczenia dokumentów, podróży i zakwaterowania. Eurojust zapewnił również urządzenia umożliwiające bezpieczną komunikację między członkami zespołu JIT. Zespół JIT przyczynił się do aresztowania około 30 wiodących podejrzanych na całym świecie, zajęcia ponad 1000 kg kokainy i aktywów wycenianych na miliony euro.

Od lutego 2011 r. w ramach Eurojustu funkcjonuje sekretariat sieci wspólnych zespołów śledczych w celu podnoszenia świadomości¹⁴, rozwiązywania problemów i wymiany najlepszych praktyk między przedstawicielami organów ścigania. Przepisy zmienionej dyrektywy w sprawie Eurojustu, które uzależniają finansowanie wspólnych zespołów dochodzeniowo-śledczych ze środków unijnych od zaproszenia Eurojustu do współpracy (art. 9f) i które zapewniają powiadamianie Eurojustu przez państwa członkowskie o utworzeniu wspólnego zespołu dochodzeniowo-śledczego (art. 13.5), ułatwią uzyskanie bardziej dokładnego przeglądu wszystkich istniejących wspólnych zespołów dochodzeniowo-śledczych w UE.

Walka z korupcją

Korupcja przez długi czas była postrzegana przede wszystkim jako problem krajowy. Z czasem jednak stało się jasne, że ma ona również skutki transgraniczne i nie może być skutecznie zwalczana w izolacji. Transgraniczna przestępczość zorganizowana często ucieka się do przekupstwa w celu ułatwienia sobie przeniknięcia systemu prawnego. Konieczne przepisy i instytucje zajmujące się korupcją zasadniczo istnieją, jednak realizacja polityki antykorupcyjnej jest w UE nierównomierna. W programie sztokholmskim wezwano Komisję do opracowania wskaźników służących do pomiaru starań państw członkowskich w walce z korupcją.

W czerwcu 2011 r. Komisja przyjęła pakiet antykorupcyjny, który ustanawia mechanizm sprawozdawczości UE („sprawozdanie o zwalczaniu korupcji w UE”) do celów okresowej oceny starań państw członkowskich w walce z korupcją. W sprawozdaniu o zwalczaniu korupcji w UE ocenie zostaną poddane osiągnięcia państw członkowskich, porażki i słabe punkty, w celu wytworzenia dodatkowej woli politycznej na rzecz wdrażania autentycznej strategii braku tolerancji dla korupcji, zachęcania do partnerskiego uczenia się i ułatwienia

¹⁴ Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością zmieniona decyzją Rady 2003/659/WSiSW i decyzją Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie wzmocnienia Eurojustu.

wymiany najlepszych praktyk. Komisja będzie publikować sprawozdanie co dwa lata, począwszy od 2013 r. Będzie się ono koncentrowało na kwestiach przekrojowych, zostaną w nim określone tendencje UE oraz przedstawione analizy dotyczące poszczególnych krajów i zalecenia.

W ramach pakietu antykorupcyjnego w sprawozdaniu Komisji na temat udziału Unii Europejskiej w Grupie Państw Przeciwko Korupcji Rady Europy (GRECO) przeanalizowano różne sposoby wzmocnienia współpracy między UE a GRECO i wysunięto wniosek, że członkostwo UE w GRECO jest odpowiednim sposobem dążenia do osiągnięcia celów programu sztokholmskiego. Na podstawie tych ustaleń Komisja złoży wniosek o upoważnienie jej przez Radę do rozpoczęcia rokowań w sprawie udziału w GRECO. Mogłoby to wytworzyć synergie między systemem oceny GRECO a sprawozdaniem o zwalczaniu korupcji w UE i zapewnić spójne podejście do walki z korupcją na szczeblu europejskim.

Przy wsparciu finansowym szczegółowego programu „Zapobieganie i walka z przestępczością” (ISEC) Transparency International przeprowadziła badanie porównawcze w Unii Europejskiej mające na celu ustalenie, czy przedawnienie ma zastosowanie do walki z korupcją (projekt zakończył się w marcu 2011 r.). Aby określić zarówno słabe punkty, jak i najlepsze praktyki w zakresie przedawnień, w badaniu przeanalizowano sytuację w 27 państwach UE (dogłębne analizy 11 państw członkowskich i ogólny zarys sytuacji w pozostałych 16). Na podstawie wyników badania Transparency International wezwie w stosownych przypadkach do przyjęcia najlepszych zidentyfikowanych praktyk¹⁵.

Konfiskata i odzyskiwanie mienia pochodzącego z działalności przestępczej

W celu odzyskiwania mienia pochodzącego z działalności przestępczej Komisja przedstawi wniosek dotyczący prawodawstwa¹⁶ mającego na celu wzmocnienie ram prawnych UE¹⁷ w zakresie konfiskaty i odzyskiwania mienia pochodzącego z działalności przestępczej w Unii Europejskiej oraz wzmocnienia wzajemnego uznawania postanowień o zabezpieczeniu i nakazów konfiskaty mienia w dziedzinie poważnych przestępstw.

Z pomocą szczegółowego programu „Zapobieganie i walka z przestępczością” UE pomaga państwom członkowskim w tworzeniu i wzmocnianiu biur ds. odzyskiwania mienia. Przykładowo, projekt w ramach programu doprowadził w 2010 r. do utworzenia węgierskiego biura ds. odzyskiwania mienia, w tym również do rozwoju nowych metod pracy na podstawie najlepszych praktyk innych państw członkowskich¹⁸. Ten i inne toczące się projekty mające na celu ułatwienie wymiany najlepszych praktyk między biurami ds. odzyskiwania mienia (np. CEART, FENIX) są regularnie prezentowane przedstawicielom organów ścigania na spotkaniach EU ARO Platform.

¹⁵ Countdown to Impunity: Corruption-related Statutes of Limitation in the European Union (EU) - JLS/2008/ISEC/100.

¹⁶ Przewidywane przyjęcie w 2012 r.

¹⁷ Decyzje ramowe 2001/500/WSISW w sprawie prania brudnych pieniędzy oraz konfiskaty, 2005/212/WSISW w sprawie rozszerzonych uprawnień do konfiskaty, 2003/577/WSISW i 2006/783/WSISW, odpowiednio w sprawie wzajemnego uznawania postanowień o zabezpieczeniu i nakazów konfiskaty mienia. .

¹⁸ Development of investigation methods and techniques in the field of asset recovery - JLS/2008/ISEC/FPA/C1/018.

Sprawozdanie z postępu prac – tabela podsumowująca wszystkie cele i działania strategii bezpieczeństwa wewnętrznego

CEL 1: Rozbijanie międzynarodowych sieci przestępczych			
	Działanie 1: Wykrywanie i rozbijanie sieci przestępczych	Działanie 2: Ochrona gospodarki przed infiltracją przestępczą	Działanie 3: Konfiskata mienia pochodzącego z działalności przestępczej
2011	<p>Wniosek w sprawie posługiwania się unijnymi danymi dotyczącymi przelotu pasażera</p>	<p>Wniosek w sprawie wsparcia dla antykorupcyjnych działań państw członkowskich oraz ich monitorowania</p> <p>Utworzenie sieci krajowych punktów kontaktowych dla organów rządowych i regulacyjnych w odniesieniu do „podejścia administracyjne go”</p>	<p>Wniosek (wnioski) Komisji dotyczący(-e) dyrektywy w sprawie konfiskaty i odzyskiwania mienia pochodzącego z działalności przestępczej i (dotyczący(-e) rozporządzenia] w sprawie stosowania zasady wzajemnego uznawania postanowień o zabezpieczeniu i nakazów konfiskaty</p>
2012	<p>Wytyczne w sprawie korzystania z rejestru rachunków bankowych dla śledzenia przepływów środków finansowych pochodzących z przestępstw</p> <p>Strategia UE w zakresie dochodzeń finansowych: zintegrowane podejście do zapobiegania, wykrywania i uniemożliwiania przenikania współczesnych zagrożeń kryminalnych do legalnej gospodarki</p>		
2013	<p>Ewentualna zmiana przepisów UE dotyczących przeciwdziałania praniu pieniędzy, by umożliwić identyfikację właścicieli spółek i funduszy powierniczych</p>		<p>Wspólne wskaźniki na potrzeby oceny działalności biur ds. odzyskiwania mienia oraz wytyczne w zakresie zapobiegania odzyskiwaniu skonfiskowanego mienia przez grupy przestępcze</p>
2014	<p>Kody kolorystyczne: <u>Zielony:</u> działanie, które (zgodnie z planem) ma zostać zakończone w 2011 r. <u>pomarańczowy:</u> działanie w toku <u>czerwony:</u> działanie nie rozpoczęte</p>		<p>Utworzenie biur ds. odzyskiwania mienia oraz niezbędne kroki dla zarządzania tym mieniem</p>

Większe wykorzystanie wspólnych zespołów dochodzeniowo-śledczych tworzonych w trybie pilnym

Działania na rzecz poprawy egzekwowania praw własności intelektualnej i zwalczania sprzedaży podrobionych towarów w Internecie

Cel 2 – Zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów

Unijna sieć upowszechniania wiedzy o radykalizacji postaw

Komisja utworzyła unijną sieć upowszechniania wiedzy o radykalizacji postaw (RAN) w współpracy z Komitetem Regionów. Inauguracji RAN dokonała komisarz Cecilia Malmström w dniu 9 września 2011 r. RAN jest unijną siecią zrzeszającą praktyków zaangażowanych w zwalczanie brutalnego ekstremizmu, w której skład wchodzi osoby odpowiedzialne za wyznaczanie kierunków polityki, funkcjonariusze organów ścigania i bezpieczeństwa, przedstawiciele władz lokalnych, przedstawiciele środowisk akademickich, eksperci terenowi i organizacje społeczeństwa obywatelskiego, w tym grupy ofiar. Do głównych celów sieci należy gromadzenie doświadczenia, wiedzy i najlepszych praktyk, a także w szczególności:

- umożliwienie komunikacji i tworzenia sieci kontaktów między członkami RAN w celu upowszechniania wiedzy o radykalizacji postaw oraz udoskonalania technik komunikacji w celu stawienia czoła retoryce terrorystycznej;
- określenie, przetestowanie, ocena i porównanie podejść oraz wyciągniętych wniosków w walce z brutalnym ekstremizmem; oraz
- informowanie decydentów zarówno na szczeblu UE, jak i państw członkowskich oraz pełnienie funkcji łącznika między Komisją a praktykami pierwszej linii;

Przy pomocy szczegółowego programu „Zapobieganie i walka z przestępczością” Komisja wspiera pracę społeczeństwa obywatelskiego i organizacji publicznych, które ujawniają, tłumaczą i podważają propagandę terrorystyczną, w tym jej przejawy w internecie.

W celu wzmocnienia współpracy operacyjnej na rzecz przeciwdziałania działalności terrorystycznej w internecie Komisja sfinansowała wiele projektów, takich jak prowadzony przez Niemcy wielostronny projekt zatytułowany „Analiza islamistycznej ekstremistycznej sieci w Europie”, który koncentruje się na treściach terrorystycznych adresowanych do młodych Europejczyków.

Ponadto środki ISEC zostały wykorzystane również do sfinansowania dialogu publiczno-prywatnego na rzecz opracowania dobrowolnego europejskiego kodeksu postępowania w zakresie najlepszych praktyk dotyczących współpracy między organami ścigania i sektorem prywatnym, w tym dostawcami usług internetowych, jak również operatorami sieci i centrami interwencji telefonicznej.

Komisja wykorzystwała również środki ISEC w celu wsparcia decydentów i zwiększenia zdolności organów ścigania UE przy pomocy szeregu badań, w tym jednego w zakresie metodyki i narzędzi technicznych służących skutecznemu wykrywaniu brutalnych treści w internecie oraz śledzenia ich autorów, którego termin zakończenia przewidywany jest na koniec 2011 r. i który pomoże w prowadzeniu śledztw i ściganiu osób odpowiedzialnych za nielegalne materiały.

Wydobywanie i analiza danych z komunikatów finansowych (TFTS UE)

UE podpisała porozumienie o programie śledzenia środków finansowych ze Stanami Zjednoczonymi (TFTP US), które zapewnia ramy prawne dla przekazywania unijnych danych z komunikatów finansowych do USA do celów walki z terroryzmem. Przeprowadzony w marcu 2011 r. przegląd wykazał skuteczność programu w walce z terroryzmem. W lipcu 2011 r. przyjęto komunikat na temat unijnego systemu śledzenia środków finansowych (TFTS), w którym opisano najważniejsze możliwe warianty utworzenia takiego systemu, a także wskazano najważniejsze kwestie wymagające rozwiązania, zanim system będzie mógł zostać formalnie zaproponowany. Celem komunikatu jest wywołanie debaty z Parlamentem Europejskim i Radą, a Komisja zaczeka z przedstawieniem wniosku ustawodawczego do momentu otrzymania wyników dyskusji.

Bezpieczeństwo transportu

Sektory morski i lotniczy wykazały już wartość dodaną, jaką odpowiednie mechanizmy komunikacji i koordynacji, jak również wspólne przepisy w dziedzinie bezpieczeństwa mogą przynieść na szczeblu UE, biorąc pod uwagę transgraniczny charakter przemysłu transportowego. Przyszły komunikat Komisji na temat bezpieczeństwa transportu będzie się koncentrował w dużym stopniu na opracowaniu podobnego unijnego podejścia do bezpieczeństwa transportu lądowego. Jego tematem przewodnim będzie też konieczność wprowadzenia odpowiednich systemów w transporcie lądowym – środków zapobiegawczych, planów postępowania awaryjnego na wypadek wystąpienia przypadków naruszenia bezpieczeństwa, planów odbudowy, szkoleń, itd. Nacisk komunikatu zostanie położony na określenie wyników w zakresie bezpieczeństwa, a nie opisowych wymogów bezpieczeństwa w dziedzinie transportu.

Aby ułatwić rozwój polityki w tym zakresie, w 2012 r. utworzona zostanie grupa doradcza ds. bezpieczeństwa transportu lądowego. Kwestie priorytetowe, którymi zajmie się grupa, obejmą konieczność wprowadzenia unijnych norm bezpieczeństwa dla sieci kolei dużych prędkości.

Sprawozdanie z postępu prac – tabela podsumowująca wszystkie cele i działania strategii bezpieczeństwa wewnętrznego

CEL 2: Zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów			
	Działanie 1: Wzmocnienie pozycji społeczeństwa w zapobieganiu radykalizacji postaw i werbowaniu terrorystów	Działanie 2: Odcięcie terrorystów od ich źródeł finansowania i materiałów oraz śledzenie dokonywanych przez nich transakcji	Działanie 3: Ochrona transportu
2011	<p>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</p>	<p>Struktury dla zamrażania aktywów terrorystów</p> <p>Struktury dla zamrażania aktywów terrorystów</p>	<p>Komunikat w sprawie polityki bezpieczeństwa transportu</p>
2012	<p>Konferencja ministerialna na temat zapobiegania radykalizacji i werbowaniu</p>		
2013	<p>Podręcznik na temat zapobiegania radykalizacji, rozbijania kanałów werbunku oraz działania na rzecz rehabilitacji i kreowania postaw negatywnych wobec terroryzmu</p>		
2014	<p>Kody kolorystyczne: Zielony: działanie, które (zgodnie z planem) ma zostać zakończone w 2011 r. pomarańczowy: działanie w toku czerwony: działanie nie rozpoczęte</p>		

Wydział planu działania na rzecz zapobiegania dostępowi do materiałów wybuchowych i substancji chemicznych, bio logicznych, radio logicznych i jądrowych

Cel 3 – Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni

Europejskie centrum ds. walki z cyberprzestępczością

Komisja zamówiła studium wykonalności odnośnie do kwestii, gdzie i jak utworzyć europejskie centrum ds. walki z cyberprzestępczością (ECC), które zgodnie z planami będzie odgrywało centralną rolę w walce z cyberprzestępczością na szczeblu europejskim. Badanie, które rozpoczęto w maju 2011 r., przyniesie wstępne wyniki przed końcem bieżącego roku. Wyniki końcowe wraz z zaleceniami będą dostępne na początku 2012 r. Z zastrzeżeniem zaleceń, jakie wynikną z badania, w czerwcu 2011 r. Europol postanowił przeorganizować swoje kompetencje w zakresie cyberprzestępczości i przesunąć zasoby na rzecz radzenia sobie z tym szybko rozwijającym się zjawiskiem.

ISEC finansuje różne projekty szkoleniowe dla organów ścigania w zakresie prowadzenia dochodzeń dotyczących cyberprzestępczości. Przykładowo w ramach projektu ISEC, który został zakończony na początku 2011 r., opracowano i przeprowadzono szkolenia dotyczące dochodzeń internetowych i kryminalistycznych. Szkolenie przeznaczone było dla pracowników różnych służb ścigania oraz podmiotów europejskich i międzynarodowych. Szczególny nacisk położono na rozwój bliższej współpracy z sektorem prywatnym. W projekcie brali udział partnerzy ze wszystkich państw członkowskich UE oraz Europol¹⁹.

Na szczeblu krajowym Komisja wspierała finansowo podnoszenie krajowej świadomości w zakresie cyberprzestępczości i rozwijanie zdolności szkoleniowych, w tym centrów doskonałości. W 2011 r. działalność rozpoczęły cztery takie centra: 2CENTRE (Francja i Irlandia), B-CENTRE (Belgia) oraz 2CENTRE EST (Estonia).

Zespoły ds. reagowania kryzysowego w dziedzinie informatycznej (CERT)

W marcu 2011 r. Komisja przyjęła komunikat w sprawie ochrony krytycznej infrastruktury teleinformatycznej²⁰, podsumowujący wykonanie planu działania na rzecz ochrony krytycznej infrastruktury teleinformatycznej na 2009 r.²¹ i opisujący kolejne kroki zarówno na szczeblu europejskim, jak i międzynarodowym. W maju 2011 r. Rada ds. Telekomunikacji przyjęła konkluzje w tym względzie. Zidentyfikowano szereg obszarów, w których konieczne są intensywniejsze starania na rzecz wzmocnienia krajowych zdolności w zakresie bezpieczeństwa cybernetycznego, zwłaszcza w odniesieniu do: utworzenia krajowych/rządowych zespołów CERT oraz utworzenia sprawnie funkcjonującej sieci krajowych/rządowych zespołów CERT w Europie do 2012 r.; opracowania krajowych planów awaryjnych na wypadek incydentów cybernetycznych oraz europejskiego planu awaryjnego na wypadek incydentów cybernetycznych; organizacji regularnych krajowych i

¹⁹ Tytuł i odniesienie: Cybercrime Investigation — Developing and disseminating an accredited international training programme for the future - JLS/2008/ISEC/FP/C4-077.

²⁰ COM(2011) 163, komunikat Komisji w sprawie ochrony krytycznej infrastruktury teleinformatycznej „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni”.

²¹ COM(2009) 149, komunikat Komisji w sprawie ochrony krytycznej infrastruktury informatycznej - „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności”.

paneuropejskich ćwiczeń na wypadek incydentów cybernetycznych. Instytucje UE poczyniły postępy w kierunku utworzenia własnych zespołów CERT, tworząc 1 czerwca 2011 r. zespół ds. wstępnej konfiguracji CERT. W ciągu 12 miesięcy zostanie on poddany ocenie, co doprowadzi do podjęcia decyzji na temat warunków utworzenia zespołu CERT dla instytucji europejskich.

Grupa robocza UE/USA w zakresie bezpieczeństwa cybernetycznego i cyberprzestępczości

Poza konkretnymi działaniami opisanymi powyżej Komisja kontynuowała ścisłą współpracę w ramach strategicznego partnerstwa w grupie roboczej UE/USA w zakresie bezpieczeństwa cybernetycznego i cyberprzestępczości, która pracuje nad ochroną kluczowych zasobów internetowych przez nadużyciami i zapobieganiem wykorzystywaniu dzieci w internecie oraz ściganiem tego procederu.

Zachowanie w internecie

Wspólnie z Europejską Służbą Działań Zewnętrznych Komisja pracuje nad ukształtowaniem europejskiego stanowiska względem najnowszych inicjatyw w zakresie zalecanego zachowania w internecie oraz umożliwienia państwom trzecim opracowania przepisów w zakresie cyberprzestępczości, tworzenia zdolności dochodzeniowych oraz doskonalenia odporności sieci w oparciu o postanowienia konwencji budapeszteńskiej o cyberprzestępczości.

Sprawozdanie z postępu prac – tabela podsumowująca wszystkie cele i działania strategii bezpieczeństwa wewnętrznego

CEL 3: Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni			
	<i>Działanie 1: Budowa zdolności w zakresie egzekwowania prawa i sądownictwa</i>	<i>Działanie 2: Współpraca z przemysłem w celu wzmocnienia pozycji obywateli i ich ochrony</i>	<i>Działanie 3: Poprawa zdolności reagowania na ataki cybernetyczne</i>
2011	<div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; width: fit-content;"> Studium wykonalności na temat unijnego centrum ds. walki z cyberprzestępczością </div>	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content;"> Wytoczne dotyczące współpracy w zwalczaniu nielegalnych treści w Internecie </div>	
2012			<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px;"> 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 </div>
2013	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content;"> Utworzenie unijnego centrum ds. walki z cyberprzestępczością </div> <div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin-left: 100px;"> Rozwój potencjału dochodzeniowo-sledczego i ścigania przestępstw w dziedzinie cyberprzestępczości </div>		<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content;"> Utworzenie europejskiego systemu ostrzegania i wymiany informacji (EISAS) </div>
2014	<div style="border: 1px solid black; background-color: #d9ead3; padding: 5px;"> <p>Kody kolorystyczne: Zielony: działanie, które (zgodnie z planem) ma zostać zakończone w 2011 r. pomarańczowy: działanie w toku czerwony: działanie nie rozpoczęte</p> </div>		
	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;"> Stworzenie mechanizmów dla zgłaszania zawiadomeń o popełnieniu cyberprzestępstwa i wyposażenie obywateli w informacje na temat bezpieczeństwa cybernetycznego i cyberprzestępczości </div>		

Cel 4 – Poprawa bezpieczeństwa poprzez zarządzanie granicami

Utworzenie EUROSUR

W 2011 r. poczyniono znaczące postępy w dalszym rozwoju i wdrażaniu EUROSUR. W styczniu 2011 r. Komisja przedstawiła ramy techniczne i operacyjne EUROSUR i zidentyfikowała działania, które należy podjąć, aby do 2013 r. EUROSUR uzyskał pełną operacyjność²². W związku z tym 16 z 18 państw członkowskich usytuowanych wzdłuż południowej granicy morskiej i wschodniej granicy lądowej UE utworzyło w 2011 r. krajowe ośrodki koordynacyjne. Jednocześnie Frontex tworzy sieć EUROSUR, która umożliwi krajowym ośrodkom koordynacyjnym i agencji Frontex wzajemną wymianę informacji w bezpieczny sposób. Po pomyślnych testach przeprowadzonych latem przez Frontex i polski krajowy ośrodek koordynacyjny Frontex rozszerzył do listopada 2011 r. sieć EUROSUR o kolejnych pięć państw członkowskich. Komisja finalizuje obecnie prace nad wnioskiem ustawodawczym dotyczącym EUROSUR, który zostanie przedstawiony Radzie w połowie grudnia 2011 r.

W kontekście EUROSUR oraz z ścisłej współpracy z COSI kilka południowych państw członkowskich rozpoczęło przygotowania do utworzenia regionalnej sieci „SEAHORSE Mediterraneo” z wybranymi afrykańskimi państwami sąsiadującymi. Jednocześnie Frontex, Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA) oraz Centrum Satelitarne UE (EUSC) opracowały wspólnie koncepcję operacji w zakresie wspólnego wykorzystywania satelitów, systemów zgłaszania statków oraz innych narzędzi nadzoru. Wybrane zastosowania tej planowanej współpracy między agencjami zostały przetestowane w toku 2011 r. przez Frontex, EMSA, EUROPOL i CeCLAD-M²³ na zachodnim Morzu Śródziemnym w ramach wspólnej operacji Frontexu Indalo. Poczyniono też postępy w dalszym rozwijaniu wspólnego mechanizmu wymiany informacji (CISE) dotyczących obszarów morskich UE.

Utworzenie wizowego systemu informacyjnego (VIS)

W 2011 r. osiągnięto znaczące postępy w zakresie finalizacji rozwoju wizowego systemu informacyjnego (VIS). Ostatnie dwa etapy testów centralnego VIS odbyły się z udziałem państw członkowskich. Tak zwane testy operacyjne systemu oraz testy tymczasowej akceptacji systemu zostały pomyślnie zakończone odpowiednio w drugim i trzecim kwartale 2011 r. Po zakończeniu tych kompleksowych testów oraz po otrzymaniu zgłoszeń gotowości wszystkich państw członkowskich biorących udział w VIS wdrażanie VIS w pierwszym regionie (Afryka Północna) rozpoczęło się dnia 11 października 2011 r. Stopniowe wdrożenie systemu w kolejnych regionach nastąpi w nadchodzących miesiącach i latach. Zarządzanie operacyjne VIS zostanie powierzone C-SIS, organowi odpowiedzialnemu za zarządzanie operacyjne SIS 1.

²² Commission staff working paper determining the technical and operational framework of EUROSUR and the actions to be taken for its establishment, SEC(2011)145 wersja ostateczna z 28.1.2011. Zob. też COM(2008)68 wersja ostateczna z 13.2.2008 i SEC(2009)1265 wersja ostateczna z 24.9.2009.

²³ Centre de Coordination pour la lutte antidrogue en Méditerranée (Ośrodek Koordynacji Walki z Narkotykami na Morzu Śródziemnym).

Wspólne zarządzanie ryzykiem przepływu towarów przez granice

Wdrożenie zmiany do kodeksu celnego dotyczącej bezpieczeństwa i ramowego systemu zarządzania ryzykiem celnym w całej UE zakończyło się w dniu 1 stycznia 2011 r. Obejmowało ono systematyczne przekazywanie zgłoszeń poprzedzających wysyłkę i przybycie towarów w podziale na sektory, elektroniczną analizę ryzyka przez unijne służby celne, wymianę komunikatów za pośrednictwem wspólnego systemu zarządzania ryzykiem celnym (CRMS) oraz program upoważnionego przedsiębiorcy. Pełne wdrożenie stanowi podstawę dla inicjatyw służących poprawie zdolności do analizy ryzyka i zapobiegania mu.

Sprawozdanie z postępu prac – tabela podsumowująca wszystkie cele i działania strategii bezpieczeństwa wewnętrznego

CEL 4: Poprawa bezpieczeństwa poprzez zarządzanie granicami				
	<i>Działanie 1: Wykorzystanie pełnego potencjału EUROSUR</i>	<i>Działanie 2: Zwiększenie wkładu Frontu w zwalczanie przestępczości na granicach zewnętrznych</i>	<i>Działanie 3: Wspólne zarządzanie ryzykiem w odniesieniu do przepływu towarów przez zewnętrzne granice UE</i>	<i>Działanie 4: Poprawa współpracy między organami krajowymi</i>
2011	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; width: 45%;">Wniosek w sprawie ustanowienia EUROSUR</div> <div style="border: 1px solid black; padding: 5px; width: 45%;">Projekt pilotażowy na południowych i południowo-zachodnich granicach UE</div> </div>	<div style="border: 1px solid black; padding: 5px; width: 100%;">Wspólne sprawozdania na temat handlu ludźmi, przemytu ludzi i przemytu nielegalnych towarów jako podstawa do wspólnych operacji</div>	<div style="border: 1px solid black; padding: 5px; width: 100%;">Inicjatywy na rzecz poprawy zdolności w zakresie określania ryzyka i jego analizy</div>	<div style="border: 1px solid black; padding: 5px; width: 100%;">Opracowanie krajowych analiz wspólnego ryzyka, obejmujących policję, straż graniczną i organy celne w celu identyfikowania niewłaściwych punktów na granicach zewnętrznych</div>
2012				<div style="border: 1px solid black; padding: 5px; width: 100%;">Propozycje dotyczące poprawy koordynacji kontroli granicznych przeprowadzanych przez różne organy</div>
2013				
2014	<div style="border: 1px solid black; padding: 5px; width: 100%;"> Kody kolorystyczne: Zielony: działanie, które (zgodnie z planem) ma zostać zakończone w 2011 r. pomarańczowy: działanie w toku czerwony: działanie nie rozpoczęte </div>			<div style="border: 1px solid black; padding: 5px; width: 100%;">Opracowanie minimalnych norm i najlepszych praktyk dla współpracy między różnymi organami</div>

Cel 5 – Zwiększenie odporności Europy na kryzysy i katastrofy

Wdrożenie klauzuli solidarności

Wdrażając klauzulę solidarności, UE stara się nadać wymierny kształt zasadzie solidarności określonej w traktacie lizbońskim (art. 222). Prace nad klauzulą solidarności rozpoczęły się.

Wytyczne dotyczące oceny ryzyka i jego mapowania w ramach zarządzania w przypadku klęsk i katastrof oraz krajowe podejścia do zarządzania ryzykiem

W celu planowanego utworzenia spójnej polityki zarządzania ryzykiem, wiążącej zagrożenie i ocenę ryzyka z procesem decyzyjnym, Komisja opracowała wraz ze wszystkimi państwami członkowskimi unijne wytyczne dotyczące oceny ryzyka i jego mapowania w ramach zarządzania w przypadku klęsk i katastrof²⁴ w oparciu o podejście ukierunkowane na wiele rodzajów zagrożenia i ryzyka, uwzględniające zasadniczo wszystkie klęski żywiołowe oraz katastrofy spowodowane przez człowieka, w tym wynikające z aktów terrorystycznych. Do końca 2011 r. państwa członkowskie powinny opracować krajowe podejścia do zarządzania ryzykiem, w tym do analizy ryzyka.

Zagrożenia dla zdrowia

Komisja Europejska rozwija inicjatywę w zakresie bezpieczeństwa zdrowia w Unii Europejskiej w celu lepszej ochrony zdrowia obywateli przed poważnymi zagrożeniami transgranicznymi. Kwestie zapobiegania zagrożeniom niesionym przez choroby zakaźne oraz ich kontroli na szczeblu UE zostały już poruszone w ustawodawstwie przyjętym w 1998 r., które stanowi podstawę dla nadzoru epidemiologicznego i koordynacji działań w sytuacjach kryzysowych. System ten od ponad dziesięciu lat dowodzi swojej skuteczności. Takie ustawodawstwo nie istnieje jednak w zakresie zagrożeń dla zdrowia ze strony substancji chemicznych i biologicznych innych niż choroby zakaźne lub zdarzenia środowiskowe. Celem tej inicjatywy jest więc rozważenie możliwości i konieczności zadbania o to, aby wszystkie rodzaje zagrożeń dla zdrowia publicznego były traktowane podobnie jak choroby zakaźne. W ramach procesu oceny skutków Komisja rozpoczęła konsultacje z zainteresowanymi podmiotami skierowane do przedstawicieli sektora zdrowia publicznego w państwach członkowskich. Wyniki konsultacji wspomogą przygotowanie inicjatywy ustawodawczej, której przedstawienie jest planowane na koniec 2011 r.²⁵.

Ochrona informacji niejawnych

UE powinna opracować zintegrowane podejście oparte na wspólnej analizie sytuacji kryzysowych i dzieleniu się spostrzeżeniami. Niektóre agencje UE odgrywają kluczowe role w tym procesie, a możliwość dzielenia się informacjami niejawnymi na odpowiednim szczeblu stanowi warunek konieczny dla lepszej wymiany informacji oraz, w stosownych przypadkach, przygotowania wspólnych unijnych sprawozdań z oceny zagrożeń i ryzyka. Skuteczna koordynacja między instytucjami, organami i agencjami UE wymaga spójnych

²⁴ Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management, SEC(2010) 1626 wersja ostateczna z 21.12.2010.

²⁵ Przewidywane przyjęcie w dniu 7 grudnia 2011 r.

ogólnych ram ochrony informacji. Komisja pracuje nad przygotowaniem spójnych ram ogólnych dla wymiany informacji niejawnych z agencjami UE, zapewniających objęcie informacji niejawnych porównywalną ochroną, jak w innych instytucjach UE i państwach członkowskich.

Europejski Potencjał Reagowania Kryzysowego

Komisja przedstawiła wniosek dotyczący ustanowienia Europejskiego Potencjału Reagowania Kryzysowego²⁶ w oparciu o wcześniej zadeklarowane zasoby państw członkowskich do wykorzystania w razie potrzeby na operacje UE i wcześniej ustalone plany awaryjne. Unia musi przejść od koordynacji *ad hoc* do systemu z góry zaplanowanego, uzgodnionego i przewidywalnego. Zwiększyłyby to skuteczność, wydajność, spójność i widoczność reagowania kryzysowego UE. Zostanie to osiągnięte w drodze szeregu działań, w tym regularnych ocen ryzyka, opracowywania scenariuszy referencyjnych, mapowania aktywów i planowania awaryjnego, utworzenia Europejskiego Potencjału Reagowania Kryzysowego w formie dobrowolnej puli środków państw uczestniczących zadeklarowanych na rzecz operacji UE, które przyczyniałyby się zarówno do planowania, jak i dostępności środków na rzecz europejskiego reagowania kryzysowego. W ramach wsparcia dla wniosku Komisji dotyczącego odnowienia przed końcem 2011 r. prawodawstwa UE w zakresie ochrony cywilnej rozpoczęto proces oceny skutków (w tym konsultacje z podmiotami zainteresowanymi).

²⁶ Komunikat Komisji – Wzmacnianie europejskiej zdolności reagowania w przypadku klęsk i katastrof: rola ochrony ludności i pomocy humanitarnej, 26.10.2010, COM(2010) 600 wersja ostateczna.

Sprawozdanie z postępu prac – tabela podsumowująca wszystkie cele i działania strategii bezpieczeństwa wewnętrznego

CEL 5: Zwiększenie odporności Europy na kryzysy i katastrofy				
	<i>Działanie 1: Pełne zastosowanie klauzuli solidarności</i>	<i>Działanie 2: Podejście do oceny zagrożenia i ryzyka przy uwzględnieniu wszystkich rodzajów zagrożenia</i>	<i>Działanie 3: Połączenie w sieć różnych ośrodków służących obserwacji położenia</i>	<i>Działanie 4: Utworzenie europejskiego potencjału reagowania w przypadku klęsk i katastrof</i>
2011	Wniosek dotyczący wdrożenia klauzuli solidarności	<p>Wytyczne dotyczące oceny ryzyka i jego mapowania w ramach zarządzania w przypadku klęsk i katastrof</p> <p>Wniosek dotyczący zagrożeń w zakresie zdrowia</p>	Wniosek w sprawie spójnych ogólnych ram dla ochrony informacji niejawnych	Wnioski w sprawie stworzenia europejskiego potencjału reagowania kryzysowego
2012		<p>Krajowe strategie zarządzania ryzykiem</p> <p>Ponadsektorowy przegląd możliwych przyszłych ryzyk naturalnych i tych wywoływanych przez człowieka</p>	Wzmocnienie powiązań pomiędzy sektorowymi systemami wczesnego ostrzegania i mechanizmami współpracy kryzysowej	
2013		Regulame przeglądy aktualnych zagrożeń		
2014	<p>Kody kolorystyczne: Zielony: działanie, które (zgodnie z planem) ma zostać zakończone w 2011 r. pomarańczowy: działanie w toku czerwony: działanie nie rozpoczęte</p>	Opracowanie spójnej polityki zarządzania ryzykiem		

Zagadnienia przekrojowe

Spójność między wewnętrznym i zewnętrznym wymiarem bezpieczeństwa

Aktualnie opracowywana jest seria inicjatyw mających na celu ułatwienie współpracy między wewnętrznymi i zewnętrznymi aspektami bezpieczeństwa. Aby zapewnić ściślejszą współpracę i koordynację w dziedzinie bezpieczeństwa UE, zwoływane będą regularne międzyinstytucjonalne spotkania informacyjne mające na celu udoskonalenie planowania i przepływu informacji w dziedzinie bezpieczeństwa UE. Pierwsze takie spotkanie między COSI i Komitetem Politycznym i Bezpieczeństwa odbyło się w dniu 1 czerwca 2011 r. w celu wymiany poglądów na temat możliwości zwiększenia synergii między wewnętrznymi i zewnętrznymi aspektami bezpieczeństwa UE. Ponadto ESDZ i Komisja sporządziły wspólny dokument dotyczący zacieśnienia więzi między podmiotami wspólnej polityki bezpieczeństwa i obrony (WPBiO) oraz wolności, bezpieczeństwa i sprawiedliwości (WSiSW), który popiera założenie, że ściślejsza współpraca między cywilnymi misjami WPBiO a podmiotami WSiSW mogłaby przynieść wymierne udoskonalenia w zakresie bezpieczeństwa UE. Szczególne zalecenia zawarte we wspólnym dokumencie podkreślają wymianę informacji jako ważną i wymagającą usprawnienia, aby znaleźć sposoby przewidywania zdarzeń zamiast reagowania na ich wystąpienie. Po drugie, należy ułatwić koordynację w planowaniu działań zewnętrznych UE, ponieważ ma ona zasadnicze znaczenie dla oddolnej współpracy w planowaniu misji.

Innym obszarem, w którym można osiągnąć wymierne rezultaty, jest współpraca między misjami policyjnymi WPBiO i Europol. Rada wielokrotnie przyznawała, że WPBiO²⁷ i szereg działań zewnętrznych WSiSW ma wspólne lub uzupełniające się cele. Misje WPBiO również w istotny sposób przyczyniły się do zwiększenia bezpieczeństwa wewnętrznego Unii, gdyż mają one na celu walkę z poważną przestępczością transgraniczną w goszczących je państwach oraz wzmocnienie przestrzegania praworządności. Rada Europejska zachęcała do ściślejszej współpracy między WSiSW i WPBiO w opracowywaniu tych wspólnych celów. Również w programie sztokholmskim przyjętym przez Radę Europejską stwierdzono, że Europol powinien ściślej współdziałać z misjami policyjnymi WPBiO i przyczynić się do promowania norm i dobrych praktyk dotyczących europejskiej współpracy w dziedzinie egzekwowania prawa w krajach spoza UE.

Szczególnie ważne z punktu widzenia obszaru WSiSW jest, aby był on zaangażowany od samego początku procesu, szczególnie podczas identyfikacji i oceny potrzeby działania UE w sytuacji kryzysowej. Umożliwi to odpowiednią i terminową ocenę niezbędnej wiedzy fachowej przy uwzględnieniu sytuacji w zakresie przestępczości zorganizowanej w danym państwie trzecim lub regionie. Pomoże to również udoskonalić decyzje polityczne i operacyjne oraz określanie zadań, które następnie będą wdrażane przez cywilne misje policyjne. Potencjał analityczny Europolu oraz należąca do niego aplikacja sieci bezpiecznej wymiany informacji (SIENA), która łączy organy ścigania wszystkich 27 państw członkowskich UE, może pomóc misjom WPBiO dostosować swoje metody i udoskonalić cele w obliczu paneuropejskiego obrazu przestępczości zorganizowanej przedstawionego przez Europol za pomocą ocen i analiz zagrożenia.

²⁷ Odniesienie do „EPBiO” (europejskiej polityki bezpieczeństwa i obrony) należy teraz odczytywać jako „WPBiO” (wspólna polityka bezpieczeństwa i obrony) w związku z wejściem w życie traktatu lizbońskiego. .

Ważnym aspektem wzajemnej współpracy jest drugi czynnik, mianowicie wymiana informacji między misjami policyjnymi WPBiO a Europolem. Mechanizm współpracy obejmujący wymianę danych nieosobowych został zasadniczo dobrze ugruntowany za pośrednictwem uzgodnień administracyjnych między Europolem a Sekretariatem Generalnym Rady. Dlatego najważniejszą kwestią jest sposób umożliwienia bezpośredniej wymiany z Europolem danych osobowych zgromadzonych przez misje policyjne WPBiO lub w związku z nimi. W przypadku EULEX Kosovo²⁸, którego mandat obejmuje również zadania wykonawcze, aby umożliwić wymianę danych osobowych z Europolem, dokonano szczególnych uzgodnień. Mechanizm ten mógłby posłużyć za przykład najlepszych praktyk i być wykorzystywany w poszczególnych przypadkach w innych misjach WPBiO. Należy ocenić potrzebę utworzenia ram ochrony danych mających zastosowanie również do WPBiO.

Polityka rozszerzenia UE w dalszym ciągu pozostaje jednym z najważniejszych elementów mających wpływ na bezpieczeństwo wewnętrzne UE. Proces rozszerzenia niesie ze sobą wiele zachęt dla państw, których on dotyczy, do przeprowadzenia reform zwiększających ich zdolności w zakresie egzekwowania prawa i sądownictwa. Ponadto dialog na temat liberalizacji systemu wizowego i mechanizm monitorowania związany z wprowadzeniem liberalizacji systemu wizowego znacząco przyczyniły się do realizacji reform w państwach Bałkanów Zachodnich.

Celem UE jest również zwiększenie zdolności państw partnerskich do odegrania swojej roli w stawieniu czoła najważniejszym obecnie zagrożeniom dla bezpieczeństwa, pokoju i stabilności na świecie. W tym celu priorytety długoterminowe określone w „Instrumencie na rzecz Stabilności” przewidują tworzenie zdolności w zakresie innowacji, łącząc pomoc techniczną i finansową na szczeblach krajowym, regionalnym i transregionalnym. Priorytet nr 1 tego instrumentu jest związany ze wsparciem na rzecz wysiłków międzynarodowych zmierzających do ograniczania zagrożeń chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ). Środki finansowane w ramach Instrumentu na rzecz Stabilności mają na celu ograniczenie zagrożeń chemicznych, biologicznych, radiologicznych i jądrowych, w tym rozprzestrzeniania broni masowego rażenia, w szczególności poprzez politykę skutecznej kontroli materiałów i środków chemicznych, biologicznych, radiologicznych i jądrowych, kontrolę wywozu towarów podwójnego zastosowania, a także ukierunkowanie naukowców zajmujących się wcześniej bronią na działania pokojowe. W okresie 2007–13 przeznaczono na ten cel 300 mln EUR, uruchomiona została też inicjatywa centrów doskonałości zajmujących się kwestiami materiałów chemicznych, biologicznych, radiologicznych i jądrowych o budżecie sięgającym blisko 100 mln EUR. Celem tej inicjatywy jest rozwój, na szczeblu krajowym i regionalnym, koniecznego potencjału instytucjonalnego w celu walki z zagrożeniem chemicznym, biologicznym, radiologicznym i jądrowym niezależnie od jego źródła: kryminalnego (rozprzestrzenianie, kradzież, sabotaż i nielegalny handel), przypadkowego (katastrofy przemysłowe, takie jak w Bhopal lub Fukushima, oraz transport) lub naturalnego (głównie pandemie).

Jeżeli chodzi o przestępczość zorganizowaną, terroryzm, nielegalny handel narkotykami, ludźmi i bronią oraz zagrożenia dla krytycznej infrastruktury, drugi priorytet Instrumentu na

²⁸ W związku z przyjęciem w dniu 17 listopada 2008 r. projektu konkluzji Rady Unii Europejskiej w sprawie ustanowienia mechanizmów współpracy w zakresie wzajemnej wymiany informacji między cywilnymi misjami realizowanymi w ramach EPBiO a Europolem wdrożona została wymiana danych osobowych między Europolem a EULEX Kosovo: dane osobowe są przekazywane między EULEX (przez EUOCI (urząd wywiadu kryminalnego Unii Europejskiej) a EUROPOL przez jednostki narodowe Europolu (ENUs) umiejscowione w trzech stolicach państw członkowskich (FI, SE, UK).

rzecz Stabilności koncentruje się na tworzeniu potencjału w ścisłych konsultacjach z państwami będącymi beneficjentami. Zazwyczaj potencjał w zakresie bezpieczeństwa jest wzmacniany na szczeblu krajowym, regionalnym, a także transregionalnym. W okresie 2007–13 na te środki przeznaczone było 118 mln EUR.

Wsparcie finansowe

Komisja pragnie zapewnić spójność działań związanych z bezpieczeństwem, w tym badań w zakresie bezpieczeństwa, polityki przemysłowej i projektów w ramach programów finansowania związanych z bezpieczeństwem wewnętrznym UE, z celami strategicznymi strategii bezpieczeństwa wewnętrznego. Środki UE, które mogą być potrzebne na okres 2012–2013, zostaną udostępnione w ramach istniejących programów finansowych („Zapobieganie i walka z przestępczością” (ISEC) oraz „Zapobieganie, gotowość i zarządzanie skutkami w zakresie terroryzmu i innych rodzajów ryzyka dla bezpieczeństwa” (CIPS). W tym względzie roczny program prac ISEC 2011 odzwierciedla obszary priorytetowe strategii bezpieczeństwa wewnętrznego w działaniu. Ponadto Komisja przeprowadziła ocenę²⁹ na podstawie uzyskanych wyników oraz jakościowych i ilościowych aspektów programu ramowego „Bezpieczeństwo i ochrona wolności (2007–2013)”, na który składają się dwa programy: ISEC i CIPS.

W okresie po 2013 r. finansowanie na rzecz bezpieczeństwa wewnętrznego zostanie przeanalizowane w kontekście debaty prowadzonej wewnątrz Komisji dotyczącej wniosków na ten okres. W ramach tej debaty Komisja przedstawiła wniosek dotyczący utworzenia w następnych wieloletnich ramach finansowych funduszu bezpieczeństwa wewnętrznego (ISF), który odzwierciedla strategiczne cele i priorytety strategii bezpieczeństwa wewnętrznego, ułatwia możliwie najlepsze wykonania działań priorytetowych przez odnośne organy krajowe i agencje, a także pozostaje wystarczająco elastyczny, aby umożliwić dostosowanie się do nowych zagrożeń i wyzwań w zakresie bezpieczeństwa. Zdaniem Komisji obecny rozdział między finansowaniem badań a środkami operacyjnymi należy zniwelować poprzez wspieranie w ramach proponowanego ISF określonych testów i prac walidacyjnych (np. prototypów systemów). Umożliwi to łatwiejsze wprowadzanie wyników wysokiej jakości badań w zakresie bezpieczeństwa do zastosowań seryjnych oraz ich wykorzystanie operacyjne na dużą skalę przez organy ścigania.

Badania w dziedzinie bezpieczeństwa i współpraca z sektorem prywatnym

Badania w zakresie bezpieczeństwa są finansowane w ramach odpowiedniego tematu siódmego programu ramowego badań (2007–2013). Komisja zapewnia ściśle dostosowanie ogólnego programowania do polityki bezpieczeństwa UE, na co wskazuje również wiele spośród ponad 200 projektów badawczych finansowanych dotychczas w ramach tego programu. Cele strategii bezpieczeństwa wewnętrznego zostały odzwierciedlone w programach prac dotyczących badań w zakresie bezpieczeństwa na lata 2011–2012. W przypadku programu prac na 2013 r., na który przeznaczono ok. 290 mln EUR, powadzona jest aktualnie analiza, która pomoże zidentyfikować najważniejsze braki i potrzeby w zakresie badań przy uwzględnieniu również priorytetów określonych w strategii bezpieczeństwa wewnętrznego w działaniu.

²⁹ Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie śródkresowej oceny programu ramowego „Bezpieczeństwo i ochrona wolności” (2007–2013), COM(2011) 318 wersja ostateczna.

Po 2013 r. badania w zakresie bezpieczeństwa będą w dalszym ciągu finansowane w ramach przyszłego wieloletniego instrumentu badań i innowacji („Horyzont 2020”). Wniosek Komisji dotyczący łącznego budżetu na badania i innowacje w następnych wieloletnich ramach finansowych zostanie zwiększony o 46%, co powinno znaleźć odzwierciedlenie w odpowiednim przydziale na rzecz badań w zakresie bezpieczeństwa.

W celu lepszego dostosowania środków związanych z bezpieczeństwem do polityki Komisja intensyfikuje również dialog prowadzony z sektorem prywatnym, w szczególności z przemysłem. W tym celu zaproponowano utworzenie regularnego (dorocznego) publiczno-prywatnego okrągłego stołu wysokiego szczebla, podczas którego instytucje unijne i organy państwa członkowskie oraz przedstawiciele sektora prywatnego mogą wymieniać się pomysłami na temat najlepszych rozwiązań w dziedzinie realizacji priorytetów strategii bezpieczeństwa wewnętrznego. Pierwszy publiczno-prywatny okrągły stół wysokiego szczebla między Unią a sektorem publicznym państw członkowskich oraz przedstawicielami sektora prywatnego odbył się w lutym 2011 r. Ponadto, aby wykorzystać potencjał w pełni funkcjonującego rynku bezpieczeństwa, Komisja przygotowuje obecnie komunikat na temat unijnej polityki w zakresie przemysłu związanego z bezpieczeństwem.