KOMISJA
EUROPEJSKA

Bruksela, dnia 29.6.2017 r.
COM(2017) 354 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa

I. WPROWADZENIE

Niniejsze sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa jest ósmym comiesięcznym sprawozdaniem i obejmuje działania w dwóch głównych dziedzinach: zwalczanie terroryzmu i przestępczości zorganizowanej oraz wspierających je środków, oraz wzmocnienie naszej obrony i odporności wobec wymienionych zagrożeń.

W ostatnich tygodniach Europa znów padła ofiarą wielu ataków terrorystycznych. W dniu 22 maja 2017 r. w Manchesterze dokonano odrażającego ataku terrorystycznego, podczas którego eksplodowała bomba przed salą koncertową, zabijając 22 osób, wśród których było wiele nastolatków. Dwanaście dni później, 3 czerwca 2017 r., Londyn został ponownie zaatakowany: terroryści wjechali w pieszych na London Bridge, a następnie pieszo kontynuowali swój zbrodniczy napad uzbrojeni w noże w okolicy Borough Market. W dniu 18 czerwca podobnego ataku przy pomocy furgonetki dokonano przed meczetem. Sprawcy zabili i ranili niewinnych wiernych. Ostatnio w dniu 19 czerwca 2017 r. terrorysta próbował napaść na funkcjonariuszy policji na Champs-Élysées w Paryżu, ale został zastrzelony. W dniu 20 czerwca 2017 r. belgijskie służby bezpieczeństwa zastrzeliły terrorystę, który usiłował dokonać samobójczego ataku bombowego na dworcu centralnym w Brukseli, jednak nie udało mu się zdetonować bomby. Liczba i częstotliwość tych ataków kolejny raz pokazują, jak wielkie znaczenie ma walka z brutalnym ekstremizmem oraz wyzwania, przed którymi stoją państwa członkowskie, by udaremniać ataki, a także zapobiegać i przeciwdziałać radykalizacji, która leży u ich podstaw.

W niniejszym sprawozdaniu przedstawiono działania podjęte na szczeblu UE w celu **zapobiegania i przeciwdziałania radykalizacji postaw**, podsumowano postępy poczynione w odpowiedzi na wyzwania związane z radykalizacją postaw w rok po przyjęciu komunikatu Komisji z czerwca 2016 r. w sprawie zapobiegania radykalizacji postaw prowadzącej do brutalnego ekstremizmu[1]. Sprawozdanie zawiera również aktualne informacje na temat postępów w realizacji innych priorytetowych działań w dziedzinie bezpieczeństwa, kolejnych kroków podjętych w celu ulepszenia **wymiany informacji** dzięki interoperacyjności systemów informacyjnych oraz wdrożenia planu działania w sprawie finansowania terroryzmu[2] w celu **wykrywania finansowania terroryzmu i zapobiegania mu**.

W konkluzjach Rady Europejskiej[3] z dn. 22–23 czerwca 2017 r. po raz kolejny podkreślono jeszcze większą determinację Unii, by współpracować na rzecz walki z rozprzestrzenianiem się radykalizacji postaw w internecie, koordynować działania w celu zapobiegania i przeciwdziałania brutalnemu ekstremizmowi i agresywnej ideologii, zająć się kwestią finansowania terroryzmu, a także ułatwić szybką i ukierunkowaną wymianę informacji między organami ścigania, w tym między zaufanymi partnerami, oraz usprawnić interoperacyjność między bazami danych. W oświadczeniu z niedawnego szczytu G7 w Taorminie[4] w sprawie zwalczania terroryzmu i brutalnego ekstremizmu stanowczo podkreślono determinację w zwalczaniu rosnącego zagrożenia terroryzmem oraz podkreślono potrzebę dalszych skoordynowanych działań na szczeblu globalnym.

---

1 COM(2016) 379 final z 14.6.2016.
2 COM(2016) 50 final z 2.2.2016.
3 http://www.consilium.europa.eu/pl/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.
4 http://www.consilium.europa.eu/pl/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

Ponadto w niniejszym sprawozdaniu poruszono kwestię **zwiększonych zagrożeń cybernetycznych** i przedstawiono krótkoterminowe działania w celu ich zwalczania w oparciu o wnioski wyciągnięte z reakcji na atak *WannaCry*.

II. DZIAŁANIA UE WSPIERAJĄCE ZAPOBIEGANIE RADYKALIZACJI POSTAW

Radykalizacja postaw prowadząca do aktów przemocy nie jest zjawiskiem nowym, jednak niedawne ataki terrorystyczne w UE wykazały niepokojące tempo i skalę radykalizacji niektórych obywateli UE. Grupy rekrutujące terrorystów stosują szereg różnych technik, za pomocą których próbują dotrzeć do osób znajdujących się w trudnej sytuacji. Wykorzystywanie narzędzi komunikacji cyfrowej stanowi nowe i szczególne wyzwanie dla organów państw członkowskich. W związku z tym przeciwdziałanie radykalizacji postaw za pośrednictwem wielopłaszczyznowej reakcji na szczeblu UE zarówno w internecie, jak i poza nim, odgrywa kluczową rolę we wspieraniu państw członkowskich w walce z terroryzmem.

W celu przecidziałania **radykalizacji postaw w internecie** Komisja współpracowała w ciągu ostatnich dwóch lat z największymi platformami internetowymi, w tym w ramach Forum UE ds. Internetu w celu zapewnienia dobrowolnego usuwania treści terrorystycznych w internecie. W ramach tych działań dokonano rzeczywistych postępów w zakresie usuwania treści terrorystycznych w internecie[5] i zwalczania nielegalnego nawoływania do nienawiści w internecie[6], ale nadal pozostaje wiele do zrobienia. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. stwierdzono że „na podstawie prac prowadzonych w ramach Forum UE ds. Internetu Rada Europejska oczekuje, że branża ustanowi forum branżowe i opracuje nowe technologie i narzędzia usprawniające automatyczne wykrywanie treści podżegających do aktów terrorystycznych i usuwanie tych treści. W razie konieczności należy to uzupełnić odpowiednimi środkami ustawodawczymi na szczeblu UE". W dniu 27 czerwca 2017 r. Komisja zorganizowała posiedzenie urzędników wyższego szczebla w ramach Forum UE ds. Internetu w celu uzgodnienia z kluczowymi dostawcami usług internetowych dalszych działań mających na celu zwalczanie treści terrorystycznych online. **Celem jest wzmocnienie działań podejmowanych przez platformy internetowe** zwłaszcza w zakresie automatycznego wykrywania treści o charakterze terrorystycznym, dzielenia się technologiami i narzędziami z mniejszymi przedsiębiorstwami, a także pełnego wykorzystywania tzw. „bazy hashów" (ang. *database of hashes*), w tym poprzez zapewnianie Europolowi dostępu do kluczowych informacji oraz ustanowienie systemu sprawozdawczości dotyczącego usuwanych treści terrorystycznych. Ponadto, w celu uzupełnienia prac prowadzonych przez jednostkę Europolu ds. zgłaszania podejrzanych treści w internecie ('jednostka IRU'), Komisja wzywa wszystkie państwa członkowskie do ustanowienia

---

[5] Za pośrednictwem **jednostki IRU** informacje o 30 000 materiałów o charakterze terrorystycznym zostały skierowane do platform internetowych, a przeciętny odsetek ich usuwania wyniósł 80–90 %. Ponadto kierowana przez branżę internetową inicjatywa dotycząca utworzenia **„bazy hashów"** gwarantuje, że materiał o charakterze terrorystycznym raz usunięty z jednej platformy nie zostanie umieszczony na innej platformie.

[6] W maju 2016 r. Komisja uzgodniła **kodeks postępowania dotyczący zwalczania nielegalnego nawoływania do nienawiści w internecie**. Kodeks ten podpisały przedsiębiorstwa Facebook, YouTube, Twitter i Microsoft, zobowiązując się do szybkiego i skutecznego przeglądu i usuwania, po uprzednim powiadomieniu, nielegalnego nawoływania do nienawiści. W ciągu roku od przyjęcia kodeks przyczynił się do osiągnięcia znacznych postępów. Przedsiębiorstwa usunęły dwukrotnie więcej treści związanych z nielegalną mową nienawiści oraz robiły to szybciej w porównaniu z okresem poprzedzającym przyjęcie kodeksu.

krajowych jednostek ds. zgłaszania podejrzanych treści w internecie oraz stworzenia sieci między nimi w celu podejmowania wspólnych działań z platformami internetowymi i jednostką IRU.

Niedawne ataki świadczą o tym, że bezprecedensowa skala radykalizacji wymaga również podjęcia dalszych działań mających na celu zapobieganie i przeciwdziałanie radykalizacji postaw na szczeblu krajowym i lokalnym. Komisja utworzy jak najszybciej[7] **grupę ekspertów wysokiego szczebla w sprawie radykalizacji postaw**, aby ułatwić dalszy rozwój polityki UE w tej dziedzinie. Zadaniem tej grupy będzie nadanie impulsu dalszym pracom w najbardziej priorytetowych dziedzinach, takich jak radykalizacja postaw w więzieniach, propaganda terrorystyczna w internecie, a także powroty zagranicznych bojowników terrorystycznych. Prace tej grupy będą ukierunkowane na wzmocnienie **sieci upowszechniania wiedzy o radykalizacji postaw („sieć RAN”)**, która odgrywa pierwszoplanową rolę w pracach Komisji mających na celu wspieranie państw członkowskich w tej dziedzinie i która współpracuje z lokalnymi specjalistami na szczeblu wspólnotowym[8]. Niedawno w dniu 19 czerwca 2017 r. w ramach sieci przedstawiono **podręcznik pt. „Responses to Returnees”** mający pomóc państwom członkowskim stawiać czoła wyzwaniom związanym z powrotami zagranicznych bojowników terrorystycznych. W podręczniku tym omówiono podejścia, jakie eksperci stosują w obliczu różnego rozwoju wydarzeń w związku z powrotami osób ze stref konfliktu. W nadchodzących miesiącach sieć zorganizuje szereg warsztatów dla władz krajowych w celu dogłębniejszego przeanalizowania tych praktyk oraz wspierania działań w państwach członkowskich.

Złożone wyzwania w zakresie radykalizacji postaw wymagają wielopłaszczyznowej reakcji, w tym środków długoterminowych, jak określono w komunikacie z czerwca 2016 r. w sprawie zapobiegania radykalizacji postaw prowadzącej do brutalnego ekstremizmu[9]. W ciągu minionego roku Komisja wdrożyła większość **kluczowych działań zidentyfikowanych w innych obszarach związanych z zapobieganiem i przeciwdziałaniem radykalizacji postaw**[10]. Mając na uwadze wspieranie państw członkowskich w przeciwdziałaniu radykalizacji postaw w więzieniach, w ramach sieci RAN utworzono grupę roboczą ds. więziennictwa i służb probacyjnych w celu zapewnienia wytycznych dla specjalistów działających w terenie, takich jak pracownicy służby więziennej i probacyjnej, psychologowie oraz przedstawiciele wspólnot religijnych. Edukacja odgrywa kluczową rolę w zapobieganiu radykalizacji, dlatego Komisja podjęła szereg kroków mających na celu wdrożenie deklaracji paryskiej w sprawie promowania – poprzez edukację – postaw obywatelskich oraz wspólnych wartości, którymi są wolność, tolerancja i

---

7 Komisja ustanowi wspomnianą grupę w lipcu 2017 r.

8 Sieć RAN zaoferowała państwom członkowskim szkolenia i doradztwo oraz opracowała szereg najlepszych praktyk, wytycznych, podręczników i zaleceń. Przedmiotowe tematy i zagadnienia obejmują programy dotyczące polaryzacji, radykalizacji postaw w więzieniach oraz wychodzenia z ekstremizmu, środków wsparcia dla rodzin, pracy z młodzieżą i edukacji, współpracy policji ze społecznością lokalną, komunikacji i narrację oraz zaangażowania i upodmiotowienia młodzieży.

9 Zob. tabela w załączniku 1 zawierająca wykaz działań podjętych w celu wdrożenia komunikatu z czerwca 2016 r.

10 W komunikacie z czerwca 2016 r. skupiono się na **siedmiu szczególnych obszarach**: (1) wspieranie badań, gromadzenie dowodów, monitorowanie i tworzenie sieci kontaktów; (2) przeciwdziałanie propagandzie terrorystycznej i nawoływaniu do nienawiści w internecie; (3) przeciwdziałanie radykalizacji w więzieniach; (4) wspieranie edukacji włączającej i promowanie wspólnych wartości UE; (5) wspieranie tworzenia integracyjnego, otwartego i odpornego społeczeństwa i docieranie do młodych ludzi; (6) aspekt przeciwdziałania radykalizacji postaw związany z bezpieczeństwem; oraz (7) wymiar międzynarodowy.

niedyskryminacja. Program Erasmus + ma kluczowe znaczenie w tym względzie[11]. Biorąc pod uwagę zależności pomiędzy marginalizacją społeczną i radykalizacją postaw, europejski filar praw socjalnych[12], przyjęty w dniu 26 kwietnia 2017 r., jest ważnym elementem w procesie eliminowania niektórych podstawowych przyczyn radykalizacji postaw i brutalnego ekstremizmu[13]. W celu zwiększenia spójności europejskich społeczeństw Komisja realizuje również plan działania na rzecz integracji obywateli państw trzecich[14] obejmujący szeroką gamę środków wspierających działania państw członkowskich i innych podmiotów na rzecz integracji.

Jeśli chodzi o **działania zewnętrzne**, UE podejmuje starania na forach międzynarodowych – zwłaszcza Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE) i instytucji[15] powiązanych ze Światowym Forum na rzecz Zwalczania Terroryzmu – w celu zapobiegania i przeciwdziałania radykalizacji postaw w krajach partnerskich w regionie Bałkanów Zachodnich, Bliskiego Wschodu i Afryki Północnej, m.in. poprzez szkolenia odpowiednich specjalistów i wsparcie finansowe dla inicjatyw oddolnych zaangażowanych w działania prewencyjne. W 2018 r. zostanie zapoczątkowana w ramach programu Erasmus+ nowa inicjatywa dotycząca wirtualnej wymiany młodzieży, której celem jest zwiększenie świadomości i zrozumienia międzykulturowego między młodzieżą w UE i poza jej granicami. Sieć upowszechniania wiedzy o radykalizacji postaw oddelegowała również ekspertów do wspierania działań prewencyjnych w Turcji, regionie Bałkanów Zachodnich i Tunezji.

III. DZIAŁANIA UE W DZIEDZINIE ZAGROŻEŃ CYBERNETYCZNYCH I CYBERPRZESTĘPCZOŚCI

W maju 2017 r. cyberatak z użyciem oprogramowania ransomware *WannaCry* był sygnałem ostrzegawczym i unaocznił luki w obecnych ramach bezpieczeństwa cybernetycznego, zwłaszcza pod względem gotowości i współpracy. Jak ogłoszono jeszcze przed zamachem w śródokresowym przeglądzie jednolitego rynku cyfrowego, **Komisja przyspiesza prace w dziedzinie bezpieczeństwa cybernetycznego**, w tym poprzez przegląd strategii bezpieczeństwa cybernetycznego z 2013 r. Komisja oraz Europejska Służba Działań Zewnętrznych dokonują oceny poczynionych postępów w realizacji obecnej strategii.

---

[11] W ramach **programu Erasmus+** w 2016 r. ponad 200 mln EUR przeznaczono na opracowanie nowych podejść i praktyk strategicznych poprzez 1200 transnarodowych projektów partnerskich, z udziałem lokalnych podmiotów i z naciskiem na edukację integracyjną, pracę z młodzieżą, obywatelstwo i edukację międzykulturową. Dla osób pracujących z młodzieżą zagrożoną radykalizacją postaw prowadzącą do aktów przemocy opracowano, we współpracy z ekspertami z państw członkowskich, nowe narzędzia zapewniające wytyczne i doradztwo. W ramach programu Erasmus + Komisja uruchomiła również **sieć wzorców zachowań**. Inicjatywa ta umożliwi podmiotom lokalnym skorzystanie z niewielkich kwot finansowania unijnego w celu opracowania zbioru wzorców zachowań w ramach działań promujących włączenie społeczne wśród uczniów i młodzieży.

[12] https://ec.europa.eu/commission/priorities/deeper-and-fairer-economic-and-monetary-union/european-pillar-social-rights/european-pillar-social-rights-20-principles_pl.

[13] W maju 2017 r. Komisja rozpoczęła konsultacje społeczne online w celu przygotowania przed końcem 2017 r. wniosku dotyczącego zalecenia Rady w sprawie propagowania włączenia społecznego i wspólnych wartości. Celem tego wniosku jest ustanowienie ram polityki wspierających państwa członkowskie w promowaniu edukacji włączającej, która promuje odpowiedzialność za wspólne wartości i tym samym przyczynia się do zapobiegania radykalizacji prowadzącej do brutalnego ekstremizmu.

[14] COM(2016) 377 final z 7.6.2016.

[15] Światowy Fundusz na rzecz Zaangażowania Społeczności i Odporności Społecznej (GCERF), centrum doskonałości Hedayah na rzecz zwalczania brutalnego ekstremizmu oraz Międzynarodowy Instytut Sprawiedliwości i Praworządności.

Działania te mają na celu stwierdzenie luk, którymi Komisja zajmie się w ramach przeglądu strategii we wrześniu 2017 r.

Równolegle do tego procesu oraz uwzględniając wnioski wyciągnięte z reakcji na atak *WannaCry*, należy obecnie podjąć szereg **krótkoterminowych działań**, aby skuteczniej reagować na coraz większe zagrożenie cybernetyczne. Oznacza to m.in. konieczność poczynienia szybkich postępów w celu zwiększenia naszej odporności, zwłaszcza w kwestiach odnoszących się do współpracy operacyjnej.

Atak *WannaCry* był pierwszym zdarzeniem, które doprowadziło do współpracy w ramach **sieci krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego** (sieć CSIRT), ustanowionej na mocy **dyrektywy o bezpieczeństwie sieci i informacji.** Incydent ten wykazał, że system nie jest jeszcze w pełni operacyjny. Unaocznił on również wyraźną potrzebę przyspieszenia trwających prac na rzecz ulepszenia istniejących narzędzi informatycznych, a także zmobilizowania dodatkowych zasobów, aby umożliwić dalszą współpracę zespołów reagowania na incydenty bezpieczeństwa komputerowego. W celu wzmocnienia tych zespołów Komisja zapewni finansowanie w wysokości 10,8 mln EUR dla 14 państw członkowskich w ramach instrumentu „Łącząc Europę", a dwuletnie projekty zostaną rozpoczęte do września 2017 r. Kolejne zaproszenie do składania wniosków jest obecnie otwarte i wszystkie pozostałe państwa członkowskie zachęca się do przedstawienia swoich wniosków o finansowanie.

Działające przy Europolu **Europejskie Centrum ds. Walki z Cyberprzestępczością** (EC3) przewodniczyło działaniom, jakie organy ścigania podjęły w reakcji na ten atak. W celu wzmocnienia tego centrum i świadczonych przez nie usług niezbędne jest wyposażenie go w dodatkową wiedzę specjalistyczną w dziedzinie IT. W tym celu zarząd Europolu powinien do września 2017 r. zwiększyć możliwości w zakresie rekrutacji specjalistów IT na mocy przepisów wewnętrznych Europolu. Działania Europolu w tym zakresie otrzymają wsparcie w 2018 r. dzięki rekrutacji dodatkowego personelu.

Zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE (CERT-UE) wspiera instytucje europejskie w zakresie ochrony przed umyślnymi i złośliwymi atakami, które mogłyby naruszyć integralność ich aktywów IT i zaszkodzić interesom UE. Komisja przyspieszy formalny proces umacniania pozycji CERT-UE poprzez zawieranie porozumień między właściwymi instytucjami i organami w celu wzmocnienia zbiorowej reakcji na zagrożenia. Są nimi Parlament Europejski, Rada, Trybunał Sprawiedliwości Unii Europejskiej, Europejski Bank Centralny, Trybunał Obrachunkowy, Europejska Służba Działań Zewnętrznych, Europejski Komitet Ekonomiczno-Społeczny, Komitet Regionów oraz Europejski Bank Inwestycyjny. Komisja podpisze wkrótce międzyinstytucjonalną umowę administracyjną z pozostałymi instytucjami i organami.

Te krótkoterminowe działania są częścią szerszego **przeglądu strategii w zakresie bezpieczeństwa cybernetycznego z 2013 r.**, który odbędzie się we wrześniu 2017 r. i któremu towarzyszyć będą konieczne działania na rzecz wzmocnienia odporności na zagrożenia cybernetyczne i bezpieczeństwa Unii. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. z zadowoleniem przyjęto fakt, że Komisja zamierza we wrześniu dokonać przeglądu strategii bezpieczeństwa cybernetycznego i przed końcem roku zaproponować kolejne ukierunkowane działania.

Skuteczne odstraszanie wymaga także skutecznych procesów identyfikowania, wykrywania, dochodzenia i ścigania. Dostęp do **elektronicznych materiałów dowodowych** ma kluczowe

znaczenie w tym względzie. Ramy wymiaru sprawiedliwości w sprawach karnych obecnie nadal odzwierciedlają tradycyjne pojęcie terytorialności i stoją przed wyzwaniem transgranicznego charakteru usług elektronicznych i przepływów danych. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. podkreślono, że skuteczny dostęp do dowodów elektronicznych ma podstawowe znaczenie dla zwalczania poważnej przestępczości i terroryzmu oraz że, z zastrzeżeniem stosownych środków ochronnych, należy zapewnić dostępność danych. Na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniu 8 czerwca 2017 r. ministrowie wyrazili szerokie poparcie dla praktycznych środków proponowanych przez Komisję w celu poprawy sytuacji w ramach aktualnych ram prawnych. Ministrowie wezwali również Komisję do przedstawienia wniosku ustawodawczego w najkrótszym możliwym terminie, biorąc pod uwagę problemy techniczne i prawne. Na tej podstawie Komisja będzie kontynuować wdrażanie praktycznych środków, a także prace nad oceną skutków ewentualnych przyszłych działań legislacyjnych, która zostanie przedstawiona w najkrótszym możliwym terminie.

Szyfrowanie jest równie ważną kwestią w tym kontekście. Ma ono zasadnicze znaczenie dla bezpieczeństwa cybernetycznego i ochrony danych osobowych. Jednak nadużywanie szyfrowania przez przestępców stwarza znaczne problemy w zakresie zwalczania poważnych form przestępczości, w tym cyberprzestępczości i terroryzmu. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. wezwano do zajęcia się problemem, jaki stanowią systemy umożliwiające terrorystom komunikowanie się przy wykorzystaniu środków, do których właściwe organy nie mają dostępu, łącznie z pełnym szyfrowaniem transmisji, przy jednoczesnym zabezpieczeniu korzyści, jakie systemy te niosą dla ochrony prywatności, danych i komunikacji. Zgodnie z wnioskiem Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych z grudnia 2016 r. Komisja ściśle współpracuje z agencjami UE i podmiotami z branży w celu zidentyfikowania sposobów wsparcia organów ścigania w przezwyciężaniu największych wyzwań, z uwzględnieniem skutków dla bezpieczeństwa cybernetycznego oraz dla praw podstawowych. Wraz z Europolem, Eurojustem, Agencją UE ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz Agencją Praw Podstawowych Unii Europejskiej Komisja omówiła wszystkie aspekty tej ważnej kwestii z odpowiednimi ekspertami podczas szeregu warsztatów. Komisja przekaże swoje ustalenia Parlamentowi Europejskiemu i Radzie w październiku 2017 r.

Odnośnie do **działań zewnętrznych**, w dniu 19 czerwca 2017 r. Rada postanowiła opracować ramy dla wspólnej reakcji dyplomatycznej UE na wrogie działania w cyberprzestrzeni (tzw. „**zestaw narzędzi dla dyplomacji cyfrowej**[16]”) Ramy wspólnych działań dyplomatycznych UE zakładają pełne wykorzystanie środków wspólnej polityki zagranicznej i bezpieczeństwa, w tym w razie potrzeby środków ograniczających. Wszelkie wspólne działania UE w odpowiedzi na wrogie działania w cyberprzestrzeni powinny być proporcjonalne do zakresu, skali, czasu trwania, intensywności, złożoności, zaawansowania i wpływu tych działań. Ramy te mają na celu zachęcanie do współpracy, ułatwienie łagodzenia bezpośrednich i długoterminowych zagrożeń oraz, w perspektywie długoterminowej, wywieranie wpływu na zachowania potencjalnych agresorów. W nadchodzących miesiącach Komisja i Europejska Służba Działań Zewnętrznych wraz z państwami członkowskimi opracują wytyczne dotyczące wdrażania, w tym praktyk przygotowawczych, procedur komunikacji i ćwiczeń.

[16] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pl/pdf.

IV. WDROŻENIE INNYCH PRIORYTETOWYCH INICJATYW DOTYCZĄCYCH BEZPIECZEŃSTWA

1. Kolejne kroki na drodze do interoperacyjności systemów informacyjnych

Jak zapowiedziano w siódmym sprawozdaniu okresowym[17], Komisja podejmie dalsze działania w celu wdrożenia nowego podejścia do zarządzania danymi dotyczącymi ochrony granic i bezpieczeństwa. W dniu 28 czerwca 2017 r. Komisja przedstawiła **wniosek[18] ustawodawczy w celu wzmocnienia mandatu agencji eu-LISA**[19]. Agencja będzie odgrywać kluczową rolę w pracach technicznych na rzecz interoperacyjności systemów informacyjnych, m.in w ramach trwającej analizy technicznej rozwiązań mających na celu osiągnięcie tego celu. Z zastrzeżeniem przyjęcia odpowiednich wniosków ustawodawczych przez współprawodawców, w wyniku proponowanych zmian do mandatu agencji eu-LISA zostanie jej powierzona odpowiedzialność za opracowanie rozwiązań w zakresie interoperacyjności technicznej, zapewniając w ten sposób techniczne wdrożenie tego nowego podejścia. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. podkreślono znaczenie interoperacyjności systemów informacyjnych dla bezpieczeństwa wewnętrznego i walki z terroryzmem.

W dniu 28 czerwca 2017 r. Komisja przedstawiła również wniosek[20] uzupełniający wniosek ze stycznia 2016 r. w celu ułatwienia **wymiany danych z rejestrów karnych na temat obywateli państw trzecich** w UE poprzez europejski system przekazywania informacji z rejestrów karnych (ECRIS)[21]. Ten uzupełniający wniosek jest odpowiedzią na dyskusje ze współprawodawcami na temat wniosku z ubiegłego roku oraz stanowi część podejścia Komisji w dziedzinie interoperacyjności systemów informacyjnych. Poprawa ECRIS w zakresie wymiany informacji dotyczących obywateli państw trzecich jest jednym z priorytetów ustawodawczych określonych we wspólnej deklaracji[22] ze spotkania przewodniczących Parlamentu Europejskiego, Rady i Komisji.

Odnotowano również **postępy w innych priorytetowych dossier dotyczących systemów informacyjnych.** Dyskusje między współprawodawcami w sprawie proponowanego unijnego systemu wjazdu/wyjazdu[23] kontynuowano w ramach posiedzeń trójstronnych, które odbyły się w dniach 31 maja oraz 13, 19 i 26 czerwca 2017 r. Rada osiągnęła porozumienie w sprawie ogólnego podejścia do proponowanego europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)[24] na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 8–9 czerwca 2017 r. Głosowanie w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego w sprawie złożonych poprawek do wniosku zaplanowano na wrzesień 2017 r., a negocjacje trójstronne powinny rozpocząć się w październiku 2017 r. Ważne jest, aby Parlament Europejski i Rada poczyniły postępy w pracach nad tymi

[17] COM(2017) 261 final z 16.5.2017.
[18] COM(2017) 352 final z 29.6.2017.
[19] Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości.
[20] COM(2016) 7 final z 19.1.2016.
[21] COM(2017) 344 final z 29.6.2017.
[22] https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.
[23] COM(2016) 194 final z 6.4.2016.
[24] COM(2016) 731 final z 16.11.2016.

priorytetowymi wnioskami, co podkreślono ponownie w konkluzjach z posiedzenia Rady Europejskiej z dn. 22–23 czerwca 2017 r.

W dniu 29 maja 2017 r. Komisja wraz z Europejskim Inspektorem Ochrony Danych, Agencją Praw Podstawowych UE oraz Koordynatorem UE ds. Zwalczania Terroryzmu przedstawili komisji LIBE ustalenia grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności[25] oraz nowe podejście Komisji do zarządzania danymi dotyczącymi ochrony granic i bezpieczeństwa. W dniu 8 czerwca 2017 r. Rada przyjęła konkluzje[26] dotyczące wymiany informacji i interoperacyjności, przyjmując z zadowoleniem opinie Komisji i proponowane sposoby osiągnięcia interoperacyjności systemów informacyjnych do 2020 r. na podstawie zaleceń grupy ekspertów wysokiego szczebla. W oparciu o te dyskusje Komisja będzie kontynuowała współpracę z Parlamentem Europejskim i Radą w celu osiągnięcia interoperacyjności systemów informacyjnych do 2020 r.

2. Działania UE w celu odcięcia źródeł i kanałów finansowania terroryzmu

Obecnie trwają prace nad wdrożeniem **planu działania z lutego 2016 r. w sprawie zwalczania finansowania terroryzmu** w dwóch głównych obszarach działań: wykrywanie finansowania terroryzmu i zapobieganie mu oraz odcinanie źródeł dochodów. W grudniu 2016 r. Komisja przedstawiła trzy wnioski legislacyjne, aby uzupełnić i wzmocnić ramy prawne UE w dziedzinie prania pieniędzy[27], nielegalnego przepływu środków pieniężnych[28] oraz zamrażania aktywów i konfiskaty mienia[29]. Komisja wzywa współprawodawców do poczynienia szybkich postępów w pracach nad tymi ważnymi wnioskami.

Ponadto współprawodawcy poczynili znaczne postępy w negocjowaniu poprawek dotyczących **4. dyrektywy w sprawie przeciwdziałania praniu pieniędzy** na podstawie wniosku ustawodawczego z lipca 2016 r[30]. Komisja pozostaje w pełni zaangażowana w przeprowadzenie szybkiej finalizacji trwających rozmów trójstronnych. Wszystkie te środki **dopełniają zobowiązań podjętych przez Komisję w planie działania**[31]. Dzięki nim UE wypełnia również swoje zobowiązania międzynarodowe w tym obszarze, podjęte w ramach Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF) oraz Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu („konwencja warszawska").

Jak zaznaczono w planie działania, Komisja zamierza przyjąć wniosek w sprawie nielegalnego handlu dobrami kultury w celu objęcia dodatkowych państw trzecich zakresem obowiązujących przepisów. Komisja rozważa również wniosek legislacyjny, który umożliwiłby organom ścigania i innym organom publicznym uzyskanie dostępu do rejestrów

---

25 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

26 Konkluzje Rady w sprawie dalszych prac nad usprawnieniem wymiany informacji i zapewnieniem interoperacyjności unijnych systemów informacyjnych: http://data.consilium.europa.eu/doc/document/ST-9448-2017-INIT/pl/pdf.

27 Wniosek dotyczący **dyrektywy w sprawie zharmonizowania definicji i sankcji karnych w odniesieniu do prania pieniędzy**, COM(2016) 826 final z 21.12.2016.

28 Wniosek dotyczący **rozporządzenia w sprawie wykrywania nielegalnych płatności gotówkowych**, COM(2016) 825 final z 21.12.2016.

29 Wniosek dotyczący **rozporządzenia w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty**, COM(2016) 819 final z 21.12.2016.

30 COM(2016) 450 final z 5.7.2016.

31 Zob. tabela w załączniku 2 zawierająca wykaz działań podjętych w celu wdrożenia planu działania z lutego 2016 r.

rachunków bankowych. Ponadto w ostatnim czasie Komisja przyjęła sprawozdanie dotyczące oceny ponadnarodowego ryzyka prania pieniędzy i finansowania terroryzmu[32], a także dokument roboczy w sprawie usprawnienia współpracy pomiędzy jednostkami analityki finansowej[33]. Jeszcze w tym roku Komisja przedstawi sprawozdanie z bieżącej oceny konieczności wprowadzenia ewentualnych dodatkowych środków mających na celu śledzenie finansowania terroryzmu w UE. Komisja prowadzi także przegląd przepisów w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi w celu uwzględnienia nowych form przestępczości i sposobów podrabiania instrumentów finansowych oraz w celu zmniejszenia częstotliwości występowania tych przestępstw oraz zniechęcenia do działalności przestępczej takiej jak finansowanie terroryzmu.

3. Wymiar zewnętrzny

W konkluzjach Rady do Spraw Zagranicznych przyjętych w dniu 19 czerwca 2017 r. w sprawie zewnętrznego wymiaru walki z terroryzmem podkreślono konieczność wzmocnienia **zewnętrznego wymiaru** zwalczania finansowania terroryzmu i prania pieniędzy[34]. W konkluzjach potwierdzono priorytety geograficzne i tematyczne dla przyszłej zewnętrznej działalności antyterrorystycznej, a mianowicie wzmocnienie współpracy w zakresie zwalczania terroryzmu z priorytetowymi państwami trzecimi Bliskiego Wschodu, Afryki Północnej, Bałkanów Zachodnich oraz Turcją, a także ze strategicznymi partnerami i organizacjami międzynarodowymi. Konkluzje zostały w znacznym stopniu zainspirowane dokumentem roboczym w sprawie zewnętrznych działań antyterrorystycznych, przedstawionym państwom członkowskim przez Europejską Służbę Działań Zewnętrznych i Komisję w maju 2017 r.

W dniu 16 czerwca 2017 r. na Malcie odbyło się **spotkanie ministrów sprawiedliwości i spraw wewnętrznych UE i USA**, które było pierwszym takim spotkaniem z udziałem nowej administracji USA. Stany Zjednoczone potwierdziły swoją chęć kontynuowania ścisłej współpracy z UE oraz podkreśliły potrzebę szybkiej wymiany informacji w ramach walki z terroryzmem i przestępczością zorganizowaną. Komisja nakreśliła działania, jakie UE podejmuje wobec zagranicznych bojowników terrorystycznych, z naciskiem na transatlantycką wymianę informacji. UE i Stany Zjednoczone przedstawiły zaktualizowane informacje w sprawie działań przeciwko radykalizacji postaw w internecie i poza nim, w sprawie zmian dotyczących danych przelotu pasażera (PNR), prania pieniędzy, zarządzania granicami i bezpieczeństwa lotnictwa. W kwestii zagrożeń dla bezpieczeństwa lotnictwa związanych z osobistymi urządzeniami elektronicznymi, UE i USA uzgodniły, że będą kontynuować współpracę w celu podnoszenia powszechnie obowiązujących norm bezpieczeństwa w lotnictwie. Komisja przekazała państwom członkowskim aktualne informacje na temat tej dyskusji oraz możliwych środków łagodzących na forum Komitetu ds. Bezpieczeństwa Lotnictwa Cywilnego w dniu 21 czerwca 2017 r. i będzie nadal ściśle współpracować z władzami Stanów Zjednoczonych na poziomie technicznym i politycznym, aby przeciwdziałać narastającym zagrożeniom.

V. PODSUMOWANIE

Niniejsze sprawozdanie koncentruje się na działaniach podjętych w ostatnich miesiącach w celu stworzenia rzeczywistej i skutecznej unii bezpieczeństwa. Wzrost liczby ataków terrorystycznych

[32] COM(2017) 340 final z 26.6.2017.
[33] SWD(2017) 275 z 26.6.2017.
[34] http://www.consilium.europa.eu/pl/press/press-releases/2017/06/19-conclusions-counterterrorism/.

w ostatnich tygodniach i miesiącach po raz kolejny przypomina o znaczeniu tych prac oraz konieczności nadania im tempa. Działania przedstawione w niniejszym sprawozdaniu wymagają pilnego wdrożenia, aby przeciwdziałać podwyższonemu zagrożeniu terrorystycznemu, zacieśniać współpracę na szczeblu UE w celu zapobiegania i przeciwdziałania radykalizacji postaw, odciąć źródła finansowania terroryzmu, zintensyfikować wymianę informacji oraz zapewnić interoperacyjność systemów informacyjnych w celu wypełnienia luk informacyjnych. W konkluzjach Rady Europejskiej z dn. 22–23 czerwca 2017 r. potwierdzono znaczenie i pilny charakter bieżących prac. Komisja wzywa Parlament Europejski i Radę do kontynuowania i wzmożenia tych wspólnych wysiłków na rzecz zwiększenia bezpieczeństwa wszystkich obywateli.

W kolejnym sprawozdaniu z postępów w realizacji unii bezpieczeństwa, planowanym na lipiec 2017 r., zostaną przedstawione wyniki kompleksowej oceny działań podejmowanych przez Unię w obszarze bezpieczeństwa wewnętrznego oraz wnioski, które Komisja wyciąga z tego pluralistycznego procesu konsultacji rozpoczętego w grudniu 2016 r.