



KOMISJA
EUROPEJSKA

WYSOKI PRZEDSTAWICIEL UNII
DO SPRAW ZAGRANICZNYCH I
POLITYKI BEZPIECZEŃSTWA

Bruksela, dnia 19.7.2017 r.
JOIN(2017) 30 final

WSPÓLNE SPRAWOZDANIE DLA PARLAMENTU EUROPEJSKIEGO I RADY

**z realizacji wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym –
odpowiedź Unii Europejskiej**

1. WPROWADZENIE

UE stoi w obliczu jednego z największych wyzwań w zakresie bezpieczeństwa w swojej historii. Zagrożenia przyjmują coraz częściej formy niekonwencjonalne, czy to w postaci przemocy fizycznej, takiej jak nowe formy terroryzmu, czy też z wykorzystaniem przestrzeni cyfrowej i złożonych ataków cybernetycznych. Inne mają formy bardziej subtelne i ukierunkowane na represyjne wywieranie nacisku, w tym dezinformujące kampanie, oraz manipulowanie mediami. Za ich pomocą próbuje się podważyć podstawowe europejskie wartości, takie jak poszanowanie godności ludzkiej, wolność i demokracja. Niedawne skoordynowane ataki cybernetyczne na całym świecie dokonane przez sprawców, których zidentyfikowanie okazało się dużym wyzwaniem, unaocznily, jak bardzo nasze społeczeństwa i instytucje są podatne na zagrożenia.

W kwietniu 2016 r. Komisja Europejska i Wysoki Przedstawiciel przyjęły wspólny komunikat w sprawie przeciwdziałania zagrożeniom hybrydowym¹ (wspólne ramy). Mając świadomość transgranicznego i złożonego charakteru zagrożeń hybrydowych, w ramach tych zaproponowano podejście zakładające zaangażowanie wszystkich władz w celu zwiększenia ogólnej odporności naszych społeczeństw na zagrożenia. Rada² z zadowoleniem przyjęła tę inicjatywę oraz proponowane działania i wezwała Komisję i Wysokiego Przedstawiciela do przedłożenia w lipcu 2017 r. sprawozdania z poczynionych postępów. UE może udzielać państwom członkowskim wsparcia w zwiększaniu przez nie ich odporności na zagrożenia hybrydowe, jednak to na państwach członkowskich spoczywa w pierwszej kolejności odpowiedzialność za przeciwdziałanie takim zagrożeniom, w zakresie, w jakim przeciwdziałanie to dotyczy bezpieczeństwa narodowego i obrony narodowej.

Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym stanowią istotną część całościowego i bardziej zintegrowanego podejścia UE do kwestii bezpieczeństwa i obrony. Stanowią one wkład w tworzenie Europy, która chroni, zgodnie z apelem wystosowanym przez przewodniczącego Jeana-Claude'a Junckera w orędziu o stanie Unii z września 2016 r. W 2016 r. Unia Europejska stworzyła również podwaliny silniejszej europejskiej polityki obrony, aby sprostać oczekiwaniom obywateli pragnących większej ochrony. W unijnej globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa UE³ przedstawiono bardziej szczegółowo konieczność zintegrowanego podejścia w celu sprzężenia wewnętrznej odporności na zagrożenia z działaniami zewnętrznymi UE i wezwano do synergii między polityką obrony a obszarami polityki dotyczącymi rynku wewnętrznego, przemysłu, organów ścigania i służb wywiadowczych. W następstwie przyjęcia w listopadzie 2016 r. europejskiego planu działań w sektorze obrony Komisja przedstawiła konkretne inicjatywy, które przyczynią się do zwiększenia zdolności UE do reagowania na zagrożenia hybrydowe dzięki zwiększeniu odporności łańcucha dostaw w sektorze obronności i wzmocnieniu jednolitego rynku wyposażenia obronnego. W szczególności w dniu 7 czerwca 2017 r. Komisja uruchomiła Europejski Fundusz Obronny, z proponowanym budżetem w wysokości 600 mln EUR do roku 2020 i 1,5 mld EUR rocznie po roku 2020. W komunikacie na temat

¹ Wspólny komunikat do Parlamentu Europejskiego i Rady *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, JOIN(2016) 18 final.

² *Konkluzje Rady w sprawie przeciwdziałania zagrożeniom hybrydowym*, komunikat prasowy 196/16 z dnia 19 kwietnia 2016 r.

³ Przedstawionej Radzie Europejskiej przez wysoką przedstawiciel w dniu 28 czerwca 2016 r.

unii bezpieczeństwa⁴ uznano konieczność przeciwdziałania zagrożeniom hybrydowym i znaczenie zapewnienia większej spójności wewnętrznych i zewnętrznych działań w dziedzinie bezpieczeństwa.

W związku z tym przywódcy UE postawili kwestie bezpieczeństwa i obrony w centrum debaty nad przyszłością Europy⁵. Potwierdzono to w deklaracji rzymskiej z dnia 25 marca 2017 r., w której przedstawiono wizję bezpiecznej Unii zdecydowanej wzmacniać swoją wspólną politykę bezpieczeństwa i obrony. W dniu 8 lipca 2016 r. przewodniczący Rady Europejskiej i Komisji Europejskiej oraz sekretarz generalny NATO podpisali w Warszawie wspólną deklarację w celu dostarczenia nowego impulsu i nowej treści strategicznemu partnerstwu między UE a NATO. We wspólnej deklaracji wskazano siedem konkretnych obszarów, w tym przeciwdziałanie zagrożeniom hybrydowym, w których współpraca między obiema organizacjami powinna zostać zacieśniona. Następnie Rady zarówno UE, jak i NATO zatwierdziły wspólny zestaw 42 propozycji realizacji tej deklaracji, a w czerwcu 2017 r. przedłożono pierwsze sprawozdanie, w którym poinformowano o poczynieniu znacznych postępów⁶.

W dokumencie dotyczącym przyszłości europejskiej obronności⁷, przedstawionym w czerwcu 2017 r., Komisja nakreśliła różne scenariusze działań w odpowiedzi na rosnące zagrożenia w zakresie bezpieczeństwa i obrony, przed jakimi stoi Europa, a także w celu zwiększenia własnych zdolności obronnych Europy do roku 2025. We wszystkich trzech scenariuszach bezpieczeństwo i obronę uznano za integralną część projektu europejskiego, niezbędną do ochrony i wspierania naszych interesów wewnętrznych i zewnętrznych. Europa musi stać się gwarantem bezpieczeństwa i przejąć stopniowo zadanie zapewniania bezpieczeństwa na swoim terytorium. Żadne państwo członkowskie nie jest w stanie w pojedynkę sprostać nadchodzącym wyzwaniom, w szczególności wyzwaniom związanym z przeciwdziałaniem zagrożeniom hybrydowym. Współpraca w dziedzinie obrony i bezpieczeństwa nie jest zatem opcją, lecz koniecznością, jeśli chcemy, by Europa zapewniała skuteczną ochronę.

Celem niniejszego sprawozdania jest przedstawienie postępów i kolejnych etapów w realizacji działań w czterech obszarach zaproponowanych we wspólnych ramach: poprawa orientacji sytuacyjnej; budowanie odporności; zwiększanie zdolności państw członkowskich i Unii do zapobiegania kryzysom i reagowania na nie, a także skoordynowanego przezwycięzania ich skutków; oraz zacieśnienie współpracy z NATO, aby zapewnić komplementarność działań. Sprawozdanie to należy odczytywać w powiązaniu z miesięcznymi sprawozdaniami z postępów na drodze ku skutecznej i rzeczywistej unii bezpieczeństwa.

⁴ COM(2016) 230 final z 20.04.2016 r.

⁵ Plan działania z Bratysławy przedstawiony przez Radę Europejską dnia 16 września 2016 r. oraz deklaracja rzymska przywódców 27 państw członkowskich i Rady Europejskiej, Parlamentu Europejskiego i Komisji Europejskiej z dnia 25 marca 2017 r.

⁶ <http://www.consilium.europa.eu/pl/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation/>

⁷ Dokument otwierający debatę na temat przyszłości europejskiej obronności, z 7.06.2017 r., https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_pl.pdf

2. ROZPOZNANIE HYBRYDOWEGO CHARAKTERU ZAGROŻENIA

Działania hybrydowe stają się coraz częstszym zjawiskiem w europejskim środowisku bezpieczeństwa. Intensywność tych działań wzrasta wraz ze wzrostem obaw dotyczących manipulacji podczas wyborów oraz wzrostem liczby kampanii dezinformacyjnych, ataków cybernetycznych przy użyciu złośliwego oprogramowania, a także prób radykalizowania szczególnie podatnych na zagrożenia członków społeczeństwa, by służyli prawdziwym sprawcom ataków hybrydowych jako „przykrywa”. Dla podatności na zagrożenia hybrydowe granice państwowe nie mają znaczenia. Zagrożenia hybrydowe wymagają skoordynowanej odpowiedzi również na szczeblu UE i NATO. Wydarzenia, jakie miały miejsce od kwietnia 2016 r., pokazały, że zagrożenia są wprowadzane nadal często oceniane w izolacji, ale wzrasta w Unii stopień świadomości i zrozumienia hybrydowego charakteru niektórych zaobserwowanych działań oraz potrzeby podjęcia skoordynowanych przeciwdziałań. UE będzie w dalszym ciągu podejmować wysiłki, aby poprawić orientację sytuacyjną i zacieśnić współpracę.

Działanie 1: Zachęca się państwa członkowskie, wspierane w stosownych przypadkach przez Komisję i Wysokiego Przedstawiciela, do przeprowadzenia badania na temat zagrożeń hybrydowych w celu rozpoznania głównych podatności na zagrożenia, w tym wskaźników dotyczących konkretnych zagrożeń hybrydowych, które mogą wpływać na krajowe i ogólnoeuropejskie struktury i sieci.

Rada powołała „Grupę Przyjaciół Prezydencji” zrzeszającą ekspertów z państw członkowskich w celu opracowania modelowego badania, które umożliwiłoby tymże państwom lepsze określenie kluczowych wskaźników dotyczących zagrożeń hybrydowych, uwzględnienie tych wskaźników w mechanizmach wczesnego ostrzegania i oceny bieżącego ryzyka oraz udostępnianie ich stosownie do potrzeb. Uzgodniono już zakres uprawnień i obowiązków grupy i rozpoczęła ona swoje prace. Modelowe badanie powinno zostać opracowane do końca 2017 r., po czym należy przystąpić w poszczególnych państwach do przeprowadzania badań na podstawie modelu. Środki ochrony przed poszczególnymi zagrożeniami hybrydowymi powinny wzajemnie się uzupełniać. Zachęca się zatem państwa członkowskie do przeprowadzenia wspomnianych badań możliwie jak najszybciej, gdyż dostarczą one cennych informacji na temat stopnia podatności na zagrożenia i gotowości w całej Europie.

a. PODNOSZENIE ŚWIADOMOŚCI

Wymiana analiz danych wywiadowczych i ocena takich danych to kluczowe narzędzia w zmniejszaniu niepewności i poprawie orientacji sytuacyjnej. W ubiegłym roku poczyniono w tym zakresie znaczne postępy. Utworzono komórkę UE ds. syntezy informacji o zagrożeniach hybrydowych, która jest już w pełni operacyjna, powołano również grupę zadaniową East Stratcom, a Finlandia uruchomiła Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych. Duża część prac ukierunkowana była na analizę narzędzi i mechanizmów szerzenia dezinformacji lub propagandy, dokonywaną przy satysfakcjonującej współpracy między grupą zadaniową UE East Stratcom, komórką UE ds. syntezy informacji o zagrożeniach hybrydowych a NATO. Stanowi to dobrą podstawę do dalszego rozwoju głębiej zakorzenionej kultury analizowania i oceny zagrożeń dla naszego bezpieczeństwa wewnętrznego i zewnętrznego pod kątem ich hybrydowego charakteru.

Komórka ds. syntezy informacji o zagrożeniach hybrydowych (ang. Hybrid Fusion Cell)

Działanie 2: Powołanie komórki UE ds. syntezy informacji o zagrożeniach hybrydowych działającej w ramach Centrum Analiz Wywiadowczych Unii Europejskiej, zdolnej do otrzymywania i analizowania informacji niejawnych, a także informacji ze źródeł jawnych na temat zagrożeń hybrydowych. Zachęca się państwa członkowskie do utworzenia krajowych punktów kontaktowych ds. zagrożeń hybrydowych, by zapewnić współpracę i bezpieczną komunikację z komórką UE ds. syntezy informacji.

Zadaniem komórki UE ds. syntezy informacji o zagrożeniach hybrydowych, utworzonej w ramach Centrum Analiz Wywiadowczych UE, jest gromadzenie i analiza informacji – zarówno niejawnych, jak i ze źródeł jawnych – dotyczących zagrożeń hybrydowych i pochodzących od różnych zainteresowanych stron. Opracowane analizy są następnie udostępniane w UE i wymieniane między państwami członkowskimi, zapewniając tym samym informacje na potrzeby procesów decyzyjnych w UE, w tym dane do celów dokonywanych na szczeblu UE ocen ryzyka w zakresie bezpieczeństwa. Dyrekcja ds. Wywiadu w Sztabie Wojskowym UE wnosi wkład w prace komórki, dostarczając analiz wojskowych. Prace nad zagrożeniami hybrydowymi zaowocowały dotychczas ponad 50 ocenami i briefingami. Od stycznia 2017 r. komórka publikuje periodyk „Biuletyn hybrydowy”, zawierający analizę bieżących zagrożeń i kwestii hybrydowych, udostępniany bezpośrednio instytucjom i jednostkom administracyjnym UE oraz krajowym punktom kontaktowym⁸. Komórka osiągnęła pełną zdolność operacyjną zgodnie z planem w maju 2017 r. Utrzymywane są również bezpośrednie kontakty z pracownikami nowo utworzonej w NATO komórki ds. analizy zagrożeń hybrydowych, polegające zarówno na dzieleniu się doświadczeniami w tworzeniu komórki analitycznej, jak i wymianie informacji (z poszanowaniem unijnych zasad dotyczących wymiany informacji niejawnych). Komórka UE ds. syntezy informacji jest obecnie w trakcie określania dalszych inicjatyw w celu usprawnienia przyszłej współpracy i odegra kluczową rolę w równoległych ćwiczeniach UE–NATO zaplanowanych na jesień 2017 r., podczas których sprawdzona zostanie jej zdolność reagowania, a zdobyte doświadczenia zostaną uwzględnione w programie jej prac.

Komunikacja strategiczna

Działanie 3: Wysoki Przedstawiciel wraz z państwami członkowskimi będzie analizować sposoby aktualizowania i koordynowania możliwości przekazywania proaktywnych komunikatów strategicznych i optymalnego wykorzystania lingwistów i specjalistów ds. monitorowania mediów.

W ostatnich miesiącach wśród szerokiego wachlarza środków stosowanych w celu osłabienia pozycji przeciwnika zwiększył się udział kampanii dezinformacyjnych i systematycznego rozpowszechniania fałszywych informacji w mediach społecznościowych. W przypadku korzystania z mediów społecznościowych jako preferowanej platformy informacji, które wydają się wiarygodne i przekonujące, mogą zmienić opinię publiczną na korzyść określonych osób, organizacji lub organów władzy. Taka taktyka hybrydowa ma szerszy cel wywołania dezorientacji w naszych społeczeństwach oraz zdyskredytowania demokratycznych władz i naszych struktur, instytucji i wyborów. Fałszywe informacje są często rozpowszechniane za pośrednictwem platform internetowych (zob. również działanie 17). Komisja i Wysoki Przedstawiciel z zadowoleniem przyjmują kroki poczynione niedawno przez platformy internetowe i wydawców mediów informacyjnych w celu przeciwdziałania

⁸ Do tej pory 21 państw członkowskich wyznaczyło krajowe punkty kontaktowe. Są to osoby pracujące w stolicach państw członkowskich, pełniące funkcje związane z polityką w tym zakresie / zwiększaniem odporności.

dezinformacji. Komisja będzie w dalszym ciągu zachęcać do wprowadzania takich dobrowolnych środków.

Wysoki Przedstawiciel powołał grupę zadaniową East Stratcom, która stara się przewidzieć przypadki i kampanie dezinformacji oraz reaguje odpowiednio w razie ich wystąpienia. Przyczynia się ona do znaczącej poprawy komunikacji na temat polityki Unii w państwach sąsiedztwa wschodniego, jednocześnie wzmacniając środowisko mediów w tych państwach. W ciągu dwóch ostatnich lat grupa zadaniowa zdemaskowała ponad 3 000 indywidualnych przypadków dezinformacji w 18 językach. Planowane wkrótce uruchomienie nowej strony internetowej: #EUvsdisinformation, zawierającej internetowe narzędzie wyszukiwania, znacznie ułatwi użytkownikom dostęp. Z badań i prac i analitycznych wynika jednak, że liczba kanałów dezinformacji i rozpowszechnianych codziennie dezinformujących wiadomości jest znacznie wyższa. W ramach projektu EU-STRAT, finansowanego ze środków programu „Horyzont 2020”, przeprowadzane są analizy polityki i mediów w państwach Partnerstwa Wschodniego.

Wysoki Przedstawiciel wzywa państwa członkowskie do wspierania prac grup zadaniowych ds. komunikacji strategicznej, aby skuteczniej przeciwdziałać wzrastającym zagrożeniom hybrydowym. Pomoże to także grupie zadaniowej South w poprawie komunikacji, również w języku arabskim, ze światem arabskim i docieraniu do niego z unijnymi przekazami, zwalczaniu szerzonych w nim mitów oraz przekazaniu faktów na temat Unii Europejskiej i jej polityki. Współpraca z lokalnymi dziennikarzami umożliwi dostosowanie przekazów informacyjnych pod względem kulturowym. Celem obu grup zadaniowych, wspieranych przez komórkę UE ds. syntezy informacji o zagrożeniach hybrydowych, jest wspomaganie i uzupełnianie wysiłków państw członkowskich w tym zakresie. Ponadto Komisja współfinansuje Europejską Sieć Komunikacji Strategicznej, sieć współpracy 26 państw członkowskich, które wymieniają się analizami, dobrymi praktykami i koncepcjami dotyczącymi wykorzystania komunikacji strategicznej w zwalczaniu brutalnego ekstremizmu, w tym kwestii dezinformacji.

Centrum doskonałości ds. zwalczania zagrożeń hybrydowych

Działanie 4: Państwa członkowskie zachęca się do rozważenia powołania centrum doskonałości ds. zwalczania zagrożeń hybrydowych.

W kwietniu 2017 r., w odpowiedzi na apel o utworzenie centrum doskonałości, Finlandia uruchomiła Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych. Członkami jest dziesięć państw członkowskich UE⁹, Norwegia i USA, przy czym zarówno Unia Europejska, jak i NATO zostały zaproszone do wkładu w prace rady kierowniczej¹⁰. Misją Centrum jest wspieranie strategicznego dialogu, a także przeprowadzanie badań i analiz we współpracy ze wspólnotami interesów w celu zwiększenia odporności i zdolności do reagowania, aby móc przeciwdziałać zagrożeniom hybrydowym. Centrum ma także służyć jako miejsce przeprowadzania w przyszłości ćwiczeń w zakresie zagrożeń hybrydowych. Centrum nawiązało już bliskie kontakty z komórką UE ds. syntezy informacji o zagrożeniach hybrydowych, a prace tych dwóch organizacji powinny się wzajemnie uzupełniać. UE analizuje obecnie sposoby udzielenia Centrum konkretnego wsparcia.

⁹ Estonia, Finlandia, Francja, Hiszpania, Litwa, Łotwa, Niemcy, Polska, Szwecja, Zjednoczone Królestwo.

¹⁰ Członkami Centrum mogą zostać również pozostałe państwa członkowskie UE i sojusznicy NATO.

b. BUDOWANIE ODPORNOŚCI

We wspólnych ramach budowaniu odporności (np. w sektorach transportu, komunikacji, energii, finansów lub w regionalnych infrastrukturach bezpieczeństwa) przyznano centralną pozycję w działaniach UE, ponieważ jest ona konieczna, aby nie ulec wpływowi propagandy i kampanii informacyjnych, a także odeprzeć próby zakłócenia funkcjonowania przedsiębiorstw, społeczeństw i przepływów ekonomicznych oraz ataki na technologie informatyczne i infrastrukturę związaną z cyberprzestrzenią. Wzmocnienie odporności uznano w nich za działanie zapobiegawcze i odstraszające, służące zespalaniu społeczeństw i zapobieganiu eskalacji kryzysów zarówno w UE, jak i poza nią. Wartością dodaną UE jest wsparcie, jakiego udziela państwom członkowskim i partnerom w zwiększaniu ich odporności, z wykorzystaniem szerokiego wachlarza istniejących instrumentów i programów. Odnotowano znaczne postępy w działaniach w celu zwiększania odporności w dziedzinach takich jak bezpieczeństwo cybernetyczne, infrastruktura krytyczna, ochrona systemu finansowego przed nielegalnym wykorzystaniem i wysiłki na rzecz przeciwdziałania brutalnemu ekstremizmowi i radykalizacji postaw.

Ochrona infrastruktury krytycznej

Działanie 5: Komisja we współpracy z państwami członkowskimi i zainteresowanymi stronami ustali wspólne narzędzia, m.in. wskaźniki, w celu poprawy ochrony i odporności infrastruktury krytycznej na wypadek zagrożeń hybrydowych w istotnych sektorach.

W ramach europejskiego programu ochrony infrastruktury krytycznej (EPCIP) Komisja podjęła prace nad określeniem wspólnych narzędzi, w tym wskaźników podatności na zagrożenia, w celu poprawy odporności infrastruktury krytycznej na zagrożenia hybrydowe w istotnych sektorach. W maju 2017 r. Komisja zorganizowała warsztaty na temat hybrydowych zagrożeń dla infrastruktury krytycznej, w których wzięli udział przedstawiciele z niemal wszystkich państw członkowskich, operatorzy infrastruktury krytycznej, przedstawiciele komórki UE ds. syntezy informacji o zagrożeniach hybrydowych oraz przedstawiciele NATO w charakterze obserwatorów. Uzgodniono wspólny plan działania i kolejne etapy przyszłych prac, w oparciu o odpowiedzi na kwestionariusz przesłany władzom krajowym w państwach członkowskich. Komisja przeprowadzi jesienią dalsze konsultacje z zainteresowanymi stronami, aby do końca 2017 r. osiągnąć porozumienie w kwestii wskaźników.

Europejska Agencja Obrony pracuje nad określeniem występujących u wszystkich stron braków w zakresie zdolności i badań, wynikających z powiązań między infrastrukturą energetyczną a zdolnościami obronnymi. Europejska Agencja Obrony opracuje jesienią 2017 r. dokument koncepcyjny, a także przedstawi działania pilotażowe służące ukształtowaniu kompleksowej metodologii.

Zwiększenie bezpieczeństwa dostaw energii w UE

Działanie 6: Komisja we współpracy z państwami członkowskimi będzie wspierać wysiłki na rzecz dywersyfikacji źródeł energii i promowania norm bezpieczeństwa w celu podniesienia poziomu odporności infrastruktury jądrowej.

W grudniu 2016 r. i w kwietniu 2017 r. Komisja przedłożyła konkretne wnioski w ramach pakietu dotyczącego bezpieczeństwa dostaw, a Rada i Parlament Europejski osiągnęły porozumienie w sprawie nowego rozporządzenia dotyczącego bezpieczeństwa dostaw gazu, którego celem jest zapobieganie kryzysom w dostawach gazu. Nowe przepisy zapewnią

koordynowane na poziomie regionalnym i wspólne podejście państw członkowskich do środków w zakresie bezpieczeństwa dostaw. Dzięki temu UE będzie mogła lepiej przygotować się na sytuacje niedoboru gazu w przypadku kryzysu lub ataku hybrydowego. Po raz pierwszy stosowana będzie zasada solidarności: państwa członkowskie będą w stanie pomóc sąsiadom w razie poważnego kryzysu lub ataku, tak aby europejskie gospodarstwa domowe i przedsiębiorstwa nie były narażone na przerwy w dostawie energii.

UE poczyniła także postępy w realizacji kluczowych projektów dotyczących dywersyfikacji dróg i źródeł dostaw energii, zgodnie ze strategią ramową na rzecz unii energetycznej oraz europejską strategią bezpieczeństwa energetycznego. Na przykład w przypadku południowego korytarza gazowego w ramach wszystkich dużych projektów budowy gazociągów prowadzone są konkretne prace budowlane: rozbudowa gazociągu południowokaukaskiego, gazociągów transanatolijskiego i transadriatyckiego, budowa gazociągu na potrzeby dostaw gazu ze złóż Shah Deniz II, jak również rozbudowa południowego korytarza gazowego na terenie Azji Środkowej, w szczególności w Turkmenistanie. Do Europy sprowadza się coraz więcej skroplonego gazu ziemnego (LNG) i to z nowych źródeł, takich jak USA. Terminal na Litwie jest dobrym przykładem na to, jak projekty w zakresie dywersyfikacji mogą przyczynić się do zmniejszenia uzależnienia od tylko jednego dostawcy. Zwiększenie wysiłków w sektorze energii i lepsze wykorzystanie rodzimych źródeł energii, zwłaszcza odnawialnych, także przyczynia się do dywersyfikacji dróg i źródeł zaopatrzenia w energię.

W dziedzinie bezpieczeństwa jądrowego Komisja aktywnie wspiera – w szczególności poprzez warsztaty z udziałem organów krajowych i regulacyjnych – spójne i skuteczne wdrażanie dyrektywy w sprawie bezpieczeństwa jądrowego oraz dyrektywy w sprawie podstawowych norm bezpieczeństwa, które państwa członkowskie mają obowiązek transponować do końca, odpowiednio, 2017 i 2018 r. Ponadto program badawczo-szkoleniowy Euratom przyczynia się do zwiększenia bezpieczeństwa jądrowego.

Bezpieczeństwo transportu i łańcucha dostaw

Działanie 7: Komisja będzie monitorować pojawiające się zagrożenia w sektorze transportu i w razie potrzeby uaktualniać przepisy. Przy wdrażaniu strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i unijnej strategii zarządzania ryzykiem celnym i związanych z nimi planów działania Komisja i Wysoki Przedstawiciel (w ramach swoich kompetencji), w koordynacji z państwami członkowskimi, zbadają, w jaki sposób należy odpowiedzieć na zagrożenia hybrydowe, zwłaszcza te dotyczące krytycznej infrastruktury transportowej.

Jak przedstawiono w komunikacie na temat unii bezpieczeństwa, Komisja udziela wsparcia w przeprowadzaniu ocen ryzyka w zakresie bezpieczeństwa na szczeblu UE, z udziałem państw członkowskich, Centrum Analiz Wywiadowczych UE i odpowiednich agencji, w celu określenia zagrożeń dla bezpieczeństwa transportu i wspierania rozwoju skutecznych i proporcjonalnych środków ograniczania ryzyka. Zestrzelenie samolotu malezyjskich linii lotniczych podczas lotu MH17 nad wschodnią Ukrainą w 2014 r. uwiaryściło ryzyko związane z przelotami nad strefami konfliktu. Zgodnie z zaleceniami europejskiej grupy zadaniowej wysokiego szczebla ds. stref konfliktu¹¹ Komisja opracowała metodę „wspólnej unijnej oceny ryzyka”, we współpracy z krajowymi ekspertami ds. lotnictwa i ds.

¹¹https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

bezpieczeństwa oraz ESDZ, umożliwiającą wymianę informacji niejawnych i definiowanie wspólnego obrazu ryzyka. W marcu 2017 r. Europejska Agencja Bezpieczeństwa Lotniczego (EASA) wydała pierwszy „Biuletyn informacyjny na temat stref konfliktu”¹², opracowany na podstawie wyników takiej wspólnej unijnej oceny ryzyka. Komisja rozważa rozszerzenie działań w zakresie oceny ryzyka prowadzonych w dziedzinie bezpieczeństwa lotniczego na inne środki transportu (np. kolej, transport morski) i przedłoży stosowne wnioski w 2018 r. W czerwcu 2017 r. Komisja, ESDZ i państwa członkowskie rozpoczęły prace nad analizą ryzyka w zakresie bezpieczeństwa kolei, w celu zidentyfikowania luk oraz określenia możliwych środków ograniczania ryzyka.

Znaczne wysiłki na rzecz ochrony lotnictwa i zarządzania ruchem lotniczym (ATM) poczyniono również w 7. programie ramowym i w projektach naukowo-badawczych w dziedzinie bezpieczeństwa w ramach programu „Horyzont 2020”. W dziedzinie lotnictwa cywilnego Komisja, we współpracy z Europejską Agencją Bezpieczeństwa Lotniczego i zainteresowanymi stronami, opracowuje dwie nowe inicjatywy w celu zwiększenia bezpieczeństwa cybernetycznego, w tym przeciwdziałania zagrożeniom hybrydowym: utworzenie zespołu reagowania na incydenty komputerowe w lotnictwie oraz powołanie grupy zadaniowej ds. bezpieczeństwa cybernetycznego we Wspólnym Przedsięwzięciu w celu Opracowania Europejskiego Systemu Zarządzania Ruchem Lotniczym Nowej Generacji (SESAR), odpowiedzialnym za zarządzanie ruchem lotniczym w jednolitej europejskiej przestrzeni powietrznej. Europejska Agencja Obrony dostarcza wojskowych informacji w zakresie cyberbezpieczeństwa w lotnictwie zarówno Wspólnemu Przedsięwzięciu SESAR, jak i Europejskiej Agencji Bezpieczeństwa Lotniczego za pośrednictwem „europejskiej strategicznej platformy koordynacyjnej ds. bezpieczeństwa cybernetycznego”, która, na wniosek państw członkowskich i przedstawicieli sektora, będzie pomagać w koordynowaniu na szczeblu unijnym wszystkich działań w dziedzinie lotnictwa. Zgodnie z planem działania dotyczącym bezpieczeństwa cybernetycznego w lotnictwie Europejska Agencja Bezpieczeństwa Lotniczego dokonała w 2016 r. analizy luk w istniejących przepisach, a w szczególności zdefiniowała zadania Europejskiego Centrum ds. Bezpieczeństwa Cybernetycznego w Lotnictwie i centrum to utworzyła; centrum rozpoczęło już swoją działalność i współpracuje z unijnym zespołem reagowania na incydenty komputerowe (CERT-UE) (protokół ustaleń podpisano w lutym 2017 r.), opracowując analizy zagrożeń w lotnictwie, oraz z organizacją EUROCONTROL (przyjęto plan działania na rzecz współpracy), ponadto uruchomiono stronę internetową służącą rozpowszechnianiu analiz informacji z otwartych źródeł. Najpóźniej jesienią 2017 r. przyjęte zostaną: program normalizacyjny i zabezpieczony system wymiany informacji.

Zarządzanie ryzykiem celnym:

W dziedzinie cel Komisja koncentruje się na zakrojonej na dużą skalę modernizacji systemu uprzedniego informowania o ładunku i zarządzania ryzykiem celnym. Obejmuje to wszelkie rodzaje ryzyka celnego, w tym w odniesieniu do zagrożeń dla bezpieczeństwa i integralności międzynarodowych łańcuchów dostaw i powiązanej infrastruktury krytycznej (np. bezpośrednie zagrożenia, jakie dla obiektów portów morskich, lotnisk lub granic lądowych stwarza import). Celem modernizacji jest zapewnienie, by organy celne w UE otrzymywały od handlowców wszelkie niezbędne informacje dotyczące przepływu towarów; by te organy w poszczególnych państwach członkowskich były w stanie skuteczniej wymieniać się tymi

¹² <https://ad.easa.europa.eu/czib-docs/page-1>

informacjami; by obok przepisów dotyczących ryzyka specyficznych dla poszczególnych państw członkowskich stosowały one również wspólne przepisy w tym zakresie; oraz by były w stanie skutecznie radzić sobie z przesłankami stwarzającymi ryzyko, dzięki bardziej intensywnej współpracy z innymi organami, w szczególności organami ścigania i agencjami bezpieczeństwa. Prace w zakresie IT konieczne do wdrożenia przez Komisję nowej wersji wspomnianego wyżej systemu są obecnie na początkowym etapie, a odnośne inwestycje na szczeblu centralnym rozpoczną się w nadchodzących miesiącach.

Przestrzeń kosmiczna

Działanie 8: W kontekście Strategii kosmicznej dla Europy i europejskiego planu działań w sektorze obrony Komisja proponuje wzmocnienie odporności infrastruktury kosmicznej na zagrożenia hybrydowe, w szczególności poprzez możliwe poszerzenie zakresu obserwacji i śledzenia obiektów kosmicznych, tak by obejmowały one zagrożenia hybrydowe, przygotowania do nowej generacji rządowej łączności satelitarnej (GOVSATCOM) na poziomie europejskim i wprowadzenie systemu Galileo do infrastruktury krytycznej zależnej od synchronizacji czasu.

Przy przygotowywaniu w 2018 r. ram regulacyjnych w zakresie rządowej łączności satelitarnej (GOVSATCOM) oraz obserwacji i śledzenia obiektów kosmicznych Komisja uwzględni w swojej ocenie kwestie odporności na zagrożenia hybrydowe. Zgodnie ze Strategią kosmiczną podczas planowania kolejnych etapów programów Galileo i Copernicus Komisja oceni możliwości wykorzystania tych usług do ograniczania stopnia podatności infrastruktury krytycznej na zagrożenia. Sprawozdanie z oceny powinno być gotowe jesienią 2017 r., a wniosek dotyczący nowej generacji programów Copernicus i Galileo – w 2018 r. Europejska Agencja Obrony pracuje nad realizowanymi na zasadzie współpracy projektami rozwoju zdolności w dziedzinie łączności satelitarnej, wojskowych systemów pozycjonowania, nawigacji i określania czasu oraz obserwacji Ziemi. Wszystkie projekty będą ukierunkowane na wymagania dotyczące odporności w świetle obecnych i rodzących się zagrożeń hybrydowych.

Zdolności obronne

Działanie 9: Wysoki Przedstawiciel, przy wsparciu – w stosownych przypadkach – ze strony państw członkowskich, we współpracy z Komisją, proponuje projekty dotyczące sposobów dostosowania zdolności obronnych oraz projekty dotyczące rozwoju mające znaczenie dla UE, w szczególności by przeciwdziałać zagrożeniom hybrydowym wymierzonym przeciwko państwu członkowskiemu lub kilku państwom członkowskim.

W latach 2016 i 2017 Europejska Agencja Obrony przeprowadziła wraz z Komisją, ESDZ i ekspertami z państw członkowskich trzy ćwiczenia symulacyjne na podstawie scenariuszy zagrożeń hybrydowych. Ich wyniki zostaną wzięte pod uwagę w przeglądzie planu rozwoju zdolności, a określone w rezultacie kierunki rozwoju kluczowych zdolności wymaganych w celu przeciwdziałania zagrożeniom hybrydowym zostaną włączone do nowych unijnych priorytetów w zakresie rozwoju zdolności. W pracach nad przeglądem katalogu potrzeb z 2005 r. uwzględniony zostanie aspekt zagrożeń hybrydowych. W kwietniu 2017 r. Europejska Agencja Obrony zakończyła prace nad sprawozdaniem analitycznym dotyczącym skutków, jakie ataki hybrydowe skierowane przeciwko krytycznej infrastrukturze portowej mogą pociągać za sobą z wojskowego punktu widzenia, które zostanie omówione podczas warsztatów z udziałem ekspertów ds. żeglugi morskiej w październiku 2017 r. Przeprowadzenie kolejnej analizy, tym razem dotyczącej roli wojska w przeciwdziałaniu zagrożeniom związanym z minidronami, zaplanowano na rok 2018. Ponadto począwszy od

2019 r. projekty dotyczące priorytetów w zakresie zdolności do wzmocnienia odporności na zagrożenia hybrydowe, określonych przez państwa członkowskie, mogą również kwalifikować się do wsparcia ze środków Europejskiego Funduszu Obrony. Komisja wzywa współprawodawców do szybkiego przyjmowania, a państwa członkowskie do składania wniosków w sprawie projektów w zakresie zdolności służących zwiększeniu odporności UE na zagrożenia hybrydowe.

Działanie 10: Komisja, we współpracy z państwami członkowskimi, zwiększy wiedzę na temat zagrożeń hybrydowych i odporność na nie w ramach istniejących mechanizmów gotowości i koordynacji, zwłaszcza w ramach Komitetu ds. Bezpieczeństwa Zdrowia.

W celu zwiększenia gotowości i odporności na zagrożenia hybrydowe, w tym rozwinięcia odpowiednich zdolności w systemach opieki zdrowotnej i systemach żywnościowych, Komisja wspiera państwa członkowskie poprzez szkolenia i ćwiczenia symulacyjne, ułatwianie wymiany doświadczeń, wytyczne oraz finansowanie wspólnych działań. Wsparcie udzielane jest w szczególności na podstawie unijnych ram bezpieczeństwa zdrowotnego w zakresie poważnych transgranicznych zagrożeń dla zdrowia oraz w ramach programu działań w dziedzinie zdrowia publicznego służącego wdrażaniu Międzynarodowych przepisów zdrowotnych – prawnego filaru, któremu podlega 196 państw, w tym państwa członkowskie, i którego celem jest zapobieganie poważnym transgranicznym zagrożeniom dla zdrowia publicznego na całym świecie i reagowanie na nie. W celu przetestowania międzysektorowej gotowości i reagowania w sektorze zdrowia służby Komisji przeprowadzą jesienią 2017 r. ćwiczenie dotyczące złożonych i wielowymiarowych zagrożeń hybrydowych. Komisja i państwa członkowskie przygotowują wspólne działanie (na lata 2018–2020) w zakresie szczepień, w tym zaopatrzenia w szczepionki i prognozowania zapotrzebowania na nie oraz badań na temat innowacyjnych procesów produkcji szczepionek, aby poprawić zaopatrzenie w szczepionki i zwiększyć bezpieczeństwo zdrowotne na szczeblu UE. Komisja współpracuje również z Europejskim Urzędem ds. Bezpieczeństwa Żywności i Europejskim Centrum ds. Zapobiegania i Kontroli Chorób w celu dostosowania się do zaawansowanych technik badań naukowych, aby móc bardziej precyzyjnie identyfikować zagrożenia dla zdrowia i ich źródła, a dzięki temu szybciej opanowywać ogniska zagrożeń dla bezpieczeństwa żywności. Ponadto Komisja stworzyła sieć podmiotów finansujących badania naukowe – światową współpracę badawczą w zakresie gotowości na wypadek wystąpienia chorób zakaźnych – w celu zapewnienia skoordynowanej reakcji badawczej w ciągu 48 godzin od wystąpienia istotnego ogniska choroby.

Działanie 11: Komisja zachęca państwa członkowskie do stworzenia – w trybie priorytetowym – i pełnego wykorzystania sieci złożonej z 28 zespołów CSIRT oraz CERT-UE (zespołu reagowania na incydenty komputerowe w instytucjach i agencjach UE), a także ram współpracy strategicznej. Komisja, w koordynacji z państwami członkowskimi, powinna dopilnować, by inicjatywy sektorowe w dziedzinie zagrożeń cybernetycznych (np. lotniczych, energetycznych, morskich) były spójne z międzysektorowymi zdolnościami objętymi zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji, takimi jak zdolność do gromadzenia informacji, łączenia wiedzy fachowej i szybkich reakcji.

Niedawne globalne ataki cybernetyczne, w których przy użyciu złośliwego oprogramowania typu ransomware zablokowano tysiące systemów komputerowych, po raz kolejny uwiarygodniły pilną potrzebę zintensyfikowania w UE działań w celu zwiększenia odporności na zagrożenia cybernetyczne i bezpieczeństwa cybernetycznego. Jak zapowiedziano w śródkresowym przeglądzie jednolitego rynku cyfrowego, Komisja i Wysoki Przedstawiciel dokonują obecnie przeglądu strategii UE w zakresie bezpieczeństwa cybernetycznego z 2013

r., w szczególności poprzez planowane na wrzesień 2017 r. przyjęcie pakietu odnośnych dokumentów. Celem przeglądu będzie zapewnienie skuteczniejszej międzysektorowej reakcji na takie zagrożenia oraz zwiększenie zaufania do społeczeństwa cyfrowego i gospodarki cyfrowej. Komisja dokona również przeglądu mandatu ENISA, Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, aby określić jej rolę w zmienionym ekosystemie cyberbezpieczeństwa. Rada Europejska¹³ z zadowoleniem przyjęła powzięty przez Komisję zamiar dokonania przeglądu strategii w zakresie bezpieczeństwa cybernetycznego.

Przyjęcie w lipcu 2016 r. dyrektywy w sprawie bezpieczeństwa sieci i informacji¹⁴ było ważnym krokiem w kierunku wzmocnienia odporności w dziedzinie bezpieczeństwa cybernetycznego na szczeblu europejskim. W dyrektywie tej ustanowiono pierwsze ogólnounijne przepisy w zakresie bezpieczeństwa cybernetycznego, zapewniono także zwiększenie zdolności w zakresie bezpieczeństwa cybernetycznego i zacieśnienie współpracy między państwami członkowskimi. Zobowiązano w niej także przedsiębiorstwa w sektorach krytycznych do wprowadzenia odpowiednich środków bezpieczeństwa i zgłaszania właściwemu organowi krajowemu wszelkich poważnych incydentów cybernetycznych. Do sektorów krytycznych zalicza się sektory: energetyki, transportu, gospodarki wodnej, opieki zdrowotnej i bankowości oraz infrastrukturę rynków finansowych. Operatorzy internetowych platform handlowych, usług przetwarzania w chmurze i wyszukiwarek internetowych będą musieli poczynić podobne kroki. Spójne wdrożenie dyrektywy w szeregu różnych sektorów, jak również w obrębie całej Unii zapewniać będzie grupa współpracy w zakresie bezpieczeństwa sieci i informacji (utworzona przez Komisję w 2016 r.), której zadaniem jest zapobiegnięcie fragmentacji rynku. W związku z tym dyrektywę w sprawie bezpieczeństwa sieci i informacji uznaje się za ramy odniesienia dla wszelkich inicjatyw sektorowych w dziedzinie bezpieczeństwa cybernetycznego. Ponadto dyrektywą tą ustanowiono sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) obejmującą wszystkie odpowiednie zainteresowane strony. Równocześnie Komisja i CERT-UE aktywnie monitorują sytuację w zakresie zagrożeń cybernetycznych i prowadzą wymianę informacji z organami krajowymi w celu zapewnienia, by systemy informatyczne instytucji unijnych były odpowiednio zabezpieczone i odporne na ataki cybernetyczne. Incydent z maja 2017 r. dotyczący wykorzystania złośliwego oprogramowania typu ransomware pod nazwą „WannaCry” był dla tej sieci pierwszą okazją do zaangażowania się w wymianę informacji operacyjnych i współpracę poprzez rozsyłanie porad. Unijny zespół reagowania na incydenty komputerowe pozostawał w bliskim kontakcie z Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) w Europolu, zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w państwach objętych atakiem, jednostkami ds. zwalczania cyberprzestępczości i kluczowymi partnerami z branży w celu ograniczenia zagrożenia i udzielenia pomocy ofiarom ataku. Dzięki wymianie krajowych sprawozdań sytuacyjnych osiągnięto wspólny poziom orientacji sytuacyjnej w całej UE. To doświadczenie umożliwiło sieci lepsze przygotowanie się na kolejne incydenty (np. ransomware pod nazwą „NonPetya”). Zidentyfikowano również szereg wyzwań i podjęto działania w celu ich pokonania.

Działanie 12: Komisja, w koordynacji z państwami członkowskimi, będzie współpracować z przemysłem w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa

¹³ Konkluzje Rady Europejskiej z dni 22–23 czerwca 2017 r.

¹⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

cybernetycznego, by rozwijać i testować technologie mające lepiej chronić użytkowników i infrastrukturę przed cybernetycznymi aspektami zagrożeń hybrydowych.

W lipcu 2016 r. Komisja, w porozumieniu z państwami członkowskimi, zawarła z przedstawicielami przemysłu umowne partnerstwo publiczno-prywatne (ang. *contractual Public Private Partnership*, cPPP) w dziedzinie bezpieczeństwa cybernetycznego, przeznaczając na nie fundusze w wysokości prawie 450 mln EUR ze środków unijnego programu ramowego w zakresie badań naukowych i innowacji „Horyzont 2020”, by rozwijać i testować technologie mające lepiej chronić użytkowników i infrastrukturę przed zagrożeniami cybernetycznymi i hybrydowymi. Partnerstwo przedstawiło pierwszy ogólnoeuropejski program badań strategicznych, w którym położono nacisk na zwiększenie odporności infrastruktury krytycznej, a także obywateli na ataki cybernetyczne. Umożliwiło ono także poprawę koordynacji między zainteresowanymi stronami, prowadzącą do wzrostu wydajności i skuteczności w wykorzystywaniu finansowania przyznawanego w ramach programu „Horyzont 2020” na projekty w zakresie bezpieczeństwa cybernetycznego. Partnerstwo prowadzi równolegle prace nad zagadnieniami związanymi z certyfikacją technologii informacyjno-komunikacyjnych dotyczącą bezpieczeństwa cybernetycznego, a także nad sposobami zaradzenia panującemu na rynku dotkliwemu niedoborowi wykwalifikowanych specjalistów w dziedzinie bezpieczeństwa cybernetycznego. Z uwagi na znaczne zapotrzebowanie na badania cywilne i wysoki poziom odporności wymagany w dziedzinie obrony grupa ds. badań naukowych i technologii cybernetycznych w Europejskiej Agencji Obrony wspiera swoim wkładem badania naukowe w dziedzinach określonych przez Europejską Organizację na rzecz Bezpieczeństwa Cybernetycznego w jej strategicznym programie badań i innowacji.

Działanie 13: Komisja wyda wytyczne dla właścicieli aktywów inteligentnych sieci w celu poprawy bezpieczeństwa cybernetycznego ich instalacji. W ramach inicjatywy dotyczącej koncepcji rynku energii elektrycznej Komisja rozważy zaproponowanie „planów gotowości na zagrożenia” oraz przepisów proceduralnych dotyczących wymiany informacji i zagwarantowania solidarności między państwami członkowskimi w czasach kryzysu, w tym zasad dotyczących sposobu zapobiegania atakom cybernetycznym i ich minimalizowania.

W sektorze energii Komisja przygotowuje strategię sektorową w zakresie bezpieczeństwa cybernetycznego, obejmującą utworzenie platformy ekspertów ds. bezpieczeństwa cybernetycznego w energetyce w celu usprawnienia wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji. Prace platformy wspomogło badanie przeprowadzone w lutym 2017 r., w którego ramach określono najlepsze dostępne techniki w celu zwiększenia poziomu bezpieczeństwa cybernetycznego inteligentnych systemów pomiarowych. Komisja stworzyła również platformę internetową „Centrum UE ds. wymiany informacji o incydentach i zagrożeniach”, służącą analizowaniu i wymianie informacji o zagrożeniach i incydentach cybernetycznych w sektorze energetycznym.

Zwiększenie odporności sektora finansowego na zagrożenia hybrydowe

Działanie 14: Komisja we współpracy z ENISA¹⁵, państwami członkowskimi oraz odnośnymi międzynarodowymi, europejskimi i krajowymi organami i instytucjami finansowymi będzie promować platformy i sieci wymiany informacji o zagrożeniach i ułatwiać ich funkcjonowanie oraz eliminować czynniki utrudniające wymianę takich informacji.

¹⁵ Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji.

Uznając zagrożenia cybernetyczne za należące do największych zagrożeń dla stabilności finansowej, Komisja dokonała przeglądu ram regulacyjnych w zakresie usług płatniczych w Unii Europejskiej, a ramy te są obecnie wdrażane. W zmienionej dyrektywie w sprawie usług płatniczych¹⁶ wprowadzono nowe przepisy w celu zwiększenia bezpieczeństwa instrumentów płatniczych i zapewnienia silnego uwierzytelniania klienta, aby ograniczyć oszustwa, zwłaszcza przy dokonywaniu płatności w internecie. Nowe ramy prawne będą miały zastosowanie od stycznia 2018 r. Komisja, wspomagana przez Europejski Urząd Nadzoru Bankowego oraz w porozumieniu z zainteresowanymi stronami, opracowuje obecnie regulacyjne standardy techniczne, które mają zostać opublikowane do końca 2017 r. i które dotyczą silnego uwierzytelniania klienta oraz opartej na wspólnych zasadach i bezpiecznej komunikacji w celu wdrożenia zabezpieczeń w transakcjach płatniczych. Ponadto na arenie międzynarodowej Komisja ściśle współpracowała z odpowiednimi partnerami z państw G-7 przy opracowywaniu wydanych przez tę grupę państw „Podstawowych zasad bezpieczeństwa cybernetycznego w sektorze finansowym”, zatwierdzonych w październiku 2016 r. przez ministrów finansów i prezesów banków centralnych państw G-7. Zasady te adresowane są do podmiotów sektora finansowego (prywatnych i publicznych) i mają przyczynić się do osiągnięcia skoordynowanego podejścia do bezpieczeństwa cybernetycznego w sektorze finansowym, aby móc wspólnie stawić czoła zagrożeniom cybernetycznym, które stają się coraz częstsze i bardziej wyrafinowane.

Transport

Działanie 15: Komisja i Wysoki Przedstawiciel (w ramach swoich kompetencji), w koordynacji z państwami członkowskimi, zbadają, w jaki sposób odpowiadać na zagrożenia hybrydowe, w szczególności te dotyczące ataków cybernetycznych w sektorze transportu.

Realizacja planu działania w ramach strategii UE w zakresie bezpieczeństwa morskiego¹⁷ pomoże odejść od mentalności izolowania się w kwestiach wymiany informacji i upowszechnić wspólne korzystanie z zasobów przez organy cywilne i wojskowe. Podejście zakładające zaangażowanie wszystkich władz zaowocowało intensywniejszą współpracą między różnymi podmiotami. Do końca 2017 r. zakończyć ma się realizacja przez Komisję i ESDZ wspólnego cywilno-wojskowego programu badań strategicznych, a ostatnie warsztaty w jego ramach poświęcone będą ochronie krytycznej infrastruktury morskiej. Prace te mogłyby w przyszłości zostać rozszerzone i objąć pojawiające się zagrożenia – w postaci ingerencji poza wodami krajowymi – dla rurociągów podwodnych, przesyłu energii, włókien światłowodowych i tradycyjnego okablowania telekomunikacyjnego.

W przeprowadzonym niedawno badaniu¹⁸ dokonano ewaluacji zdolności krajowych organów pełniących funkcje straży przybrzeżnej do oceny ryzyka. Określono w nim najważniejsze przeszkody utrudniające współpracę w tym zakresie między organami morskimi na szczeblu UE i krajowym oraz zalecane praktyczne sposoby usprawnienia jej. Ocena ryzyka ma

¹⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (Dz.U. L 337 z 23.12.2015, s. 35).

¹⁷ https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf oraz drugie sprawozdanie z realizacji planu działania w ramach strategii UE w zakresie bezpieczeństwa morskiego, przedłożone państwom członkowskim w dniu 21 czerwca 2017 r.

¹⁸ Badanie z 2017 r. „Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions” (Ewaluacja zdolności oceny ryzyka na szczeblu organów państw członkowskich pełniących funkcje straży przybrzeżnej), <https://ec.europa.eu/maritimeaffairs/documentation/studies>

zasadnicze znaczenie w przeciwdziałaniu zagrożeniom na morzu, a jeszcze bardziej kluczowa jest dla ewaluacji zagrożeń hybrydowych i zapobiegania im, ponieważ wymagają one dodatkowych i bardziej złożonych analiz. Wyniki wspomnianego badania zostaną przedstawione na różnych forach ds. straży przybrzeżnej, tak aby proponowane zalecenia mogły zostać ocenione i wdrożone w celu zacieśnienia współpracy w tym obszarze, głównie z myślą o poprawie gotowości i reagowania na zagrożenia hybrydowe.

Zwalczanie finansowania terroryzmu

Działanie 16: Wdrożenie planu działania w sprawie zwalczania finansowania terroryzmu także posłuży Komisji do przeciwdziałania zagrożeniom hybrydowym.

Sprawcy ataków hybrydowych i ich poplecznicy potrzebują środków finansowych do realizacji swoich planów. Wysiłki UE skierowane przeciwko finansowaniu przestępczości i terroryzmu, podejmowane zgodnie z Europejską agendą bezpieczeństwa i planem działania na rzecz zwalczania finansowania terroryzmu, mogą więc przyczynić się również do przeciwdziałania zagrożeniom hybrydowym. W grudniu 2016 r. Komisja przedstawiła trzy wnioski ustawodawcze dotyczące między innymi sankcji karnych za pranie pieniędzy i nielegalne płatności gotówkowe, jak również zabezpieczania i konfiskaty mienia¹⁹. Wszystkie państwa członkowskie miały obowiązek transponować czwartą dyrektywę w sprawie przeciwdziałania praniu pieniędzy²⁰ do dnia 26 czerwca 2017 r., a w lipcu 2016 r. Komisja przedłożyła specjalny wniosek ustawodawczy w celu uzupełnienia tej dyrektywy dodatkowymi środkami²¹ i zaostrzenia jej przepisów.

W dniu 26 czerwca 2017 r. Komisja wydała ponadnarodową ocenę ryzyka, przewidzianą w czwartej dyrektywie w sprawie przeciwdziałania praniu pieniędzy. Komisja przedłożyła również wniosek dotyczący rozporządzenia w celu zapobiegania przywozowi do UE i przechowywaniu w UE dóbr kultury nielegalnie wywiezionych z państw trzecich²². Jeszcze w tym roku Komisja przedstawi sprawozdanie z trwającej obecnie oceny potrzeby wprowadzenia ewentualnych dodatkowych środków służących wykrywaniu finansowania terroryzmu w UE. Komisja prowadzi również przegląd przepisów w zakresie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi²³.

W ósmym sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa zawarto więcej informacji na temat stanu wdrożenia planu działania na rzecz zwalczania finansowania terroryzmu.

Propagowanie wspólnych wartości UE i sprzyjających włączeniu społecznemu, otwartych i odpornych na zagrożenia społeczeństw

¹⁹ Trzecie sprawozdanie z postępów ku skutecznej i rzeczywistej unii bezpieczeństwa (COM(2016) 831 final).

²⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. L 141 z 5.6.2015, s. 73–117).

²¹ Więcej informacji na ten temat można znaleźć w komunikatach: „Trzecie sprawozdanie z postępów ku skutecznej i rzeczywistej unii bezpieczeństwa” (COM(2016) 831 final) i „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa” (COM(2017) 354 final).

²² COM(2017) z 26.06.2017 r., COM(2017) 340 final, SWD(2017) 275 final 0.

²³ Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 354 final).

Budowanie odporności w obliczu radykalizacji postaw i brutalnego ekstremizmu

Radykalizacja religijna i ideologiczna, konflikty etniczne i konflikty na tle mniejszościowym mogą być inicjowane przez podmioty zewnętrzne przy pomocy określonych grup lub poprzez działania podsycające konflikty między grupami. Pojawiły się także dodatkowe wyzwania, takie jak zagrożenia ze strony sprawców działających w pojedynkę, nowe metody radykalizowania, w tym możliwe wykorzystanie w tym celu kryzysu migracyjnego, jak również wzrost prawicowego ekstremizmu (w tym przemocy wobec migrantów) i ryzyko związane z polaryzacją społeczeństw. Przeciwdziałaniem radykalizacji zajęto się w ramach unii bezpieczeństwa, może być ono jednak pośrednio istotne z perspektywy zagrożeń hybrydowych, gdyż osoby podatne na radykalizację mogą paść ofiarami manipulacji ze strony sprawców ataków hybrydowych.

Działanie 17: Komisja wdraża działania przeciwko radykalizacji postaw określone w Europejskiej agendzie bezpieczeństwa i analizuje potrzebę wzmocnienia procedur usuwania nielegalnych treści, wzywając pośredników do zachowania należytej staranności podczas zarządzania swoimi sieciami i systemami.

Zapobieganie radykalizacji

Komisja kontynuuje wdrażanie swojej wielopłaszczyznowej reakcji na radykalizację, przedstawionej w wydanym w czerwcu 2016 r. komunikacie w sprawie zapobiegania radykalizacji postaw prowadzącej do brutalnego ekstremizmu²⁴, w którym określono kluczowe działania, takie jak propagowanie edukacji sprzyjającej włączeniu społecznemu i wspólnych wartości, zwalczanie propagandy ekstremistycznej w internecie i radykalizacji postaw w zakładach karnych, zacieśnienie współpracy z państwami trzecimi oraz intensyfikacja badań naukowych w celu lepszego zrozumienia zmieniającego się charakteru radykalizacji postaw i lepszego wykorzystania tej wiedzy do kształtowania strategii politycznych. Czołową inicjatywą Komisji służącą wspieraniu państw członkowskich w tym zakresie jest sieć upowszechniania wiedzy o radykalizacji postaw (ang. Radicalisation Awareness Network, RAN), pracująca z lokalnymi ekspertami na szczeblu społeczności. Więcej informacji na ten temat zawarto w komunikacie „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”²⁵.

Radykalizacja w internecie i nawoływanie do nienawiści

Zgodnie z Europejską agendą bezpieczeństwa²⁶ Komisja poczyniła kroki w celu ograniczenia dostępności nielegalnych treści w internecie, w szczególności przy pomocy działającej w Europolu unijnej jednostki ds. zgłaszania podejrzanych treści w internecie oraz internetowego forum UE²⁷. Znaczne postępy poczyniono również dzięki wprowadzeniu kodeksu

²⁴ http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

²⁵ COM(2017) 354 final.

²⁶ Więcej informacji można znaleźć w komunikacie „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”, COM(2017) 354 final.

²⁷ Więcej informacji można znaleźć w komunikacie „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”, COM(2017) 354 final.

postępowania w zakresie zwalczania nawoływania do nienawiści w internecie²⁸. Więcej informacji na ten temat zawarto w komunikacie „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”²⁹. Działania te zostaną zintensyfikowane, również w świetle konkluzji Rady Europejskiej³⁰, szczytu G-7³¹ oraz szczytu G-20 w Hamburgu³².

Platformy internetowe odgrywają kluczową rolę w zwalczaniu nielegalnych lub potencjalnie szkodliwych treści. W ramach strategii jednolitego rynku cyfrowego, jak określono w przeglądzie śródkresowym³³, Komisja zapewni lepszą koordynację dialogów z platformami, koncentrując się na zagadnieniu mechanizmów i rozwiązań technicznych służących usuwaniu nielegalnych treści. W stosownych przypadkach należy dążyć do zapewnienia takim mechanizmom podbudowy w postaci wytycznych dotyczących kwestii takich jak zgłaszanie i usuwanie nielegalnych treści. Komisja opracuje również wytyczne dotyczące zasad odpowiedzialności.

Zacieśnienie współpracy z państwami trzecimi

Działanie 18: Wysoki Przedstawiciel, we współpracy z Komisją, przeprowadzi analizę zagrożenia hybrydowego w sąsiednich regionach. Wysoki Przedstawiciel, Komisja i państwa członkowskie zastosują instrumenty będące do ich dyspozycji w celu zbudowania zdolności partnerów i wzmocnienia ich odporności na zagrożenia hybrydowe. Można realizować misje WPBiO, niezależnie od instrumentów unijnych lub jako ich uzupełnienie, aby wspomóc partnerów w rozwijaniu ich zdolności.

Unia Europejska kładzie większy nacisk na budowanie zdolności i odporności w krajach partnerskich w sektorze bezpieczeństwa, m.in. wykorzystując powiązania między bezpieczeństwem a rozwojem, dbając o to, by zmieniona europejska polityka sąsiedztwa w większym stopniu uwzględniała kwestię bezpieczeństwa oraz podejmując dialogi dotyczące zwalczania terroryzmu i zapewniania bezpieczeństwa z państwami w basenie Morza Śródziemnego. W tym celu w ramach projektu pilotażowego przeprowadzono badanie na temat zagrożeń, we współpracy z Republiką Mołdawii. Badanie to ma pomóc w identyfikacji głównych podatności na zagrożenia w danym państwie oraz zapewnić, by wsparcie UE ukierunkowane było na działania właśnie w tych obszarach. Wyniki projektu pilotażowego wskazują, że samo badanie zostało uznane za użyteczne. W oparciu o zdobyte doświadczenia Komisja i ESDZ wydadzą zalecenia priorytetowego traktowania działań na rzecz zwiększania skuteczności oraz rozwoju komunikacji strategicznej, ochrony infrastruktury krytycznej i bezpieczeństwa cybernetycznego.

W oparciu o te pierwsze doświadczenia w przyszłości kolejne państwa sąsiadujące mogłyby skorzystać ze wspomnianego badania, dostosowanego jednak odpowiednio, tak by odzwierciedlić zróżnicowane krajowe uwarunkowania lokalne i specyficzne zagrożenia, a

²⁸ Kodeks postępowania w zakresie zwalczania nawoływania do nienawiści w internecie, z 31 maja 2016 r., http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

²⁹ Więcej informacji można znaleźć w komunikacie „Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”, COM(2017) 354 final.

³⁰ Konkluzje Rady Europejskiej z dni 22–23 czerwca 2017 r.

³¹ Szczyt G-7 w Taorminie (Włochy), 26–27.05.2017.

³² Szczyt G-20 w Hamburgu (Niemcy), 7–8.07.2017.

³³ Por. komunikat Komisji COM(2017) 228 final.

także uniknąć powielania działań prowadzonych w ramach toczących się dialogów dotyczących zwalczania terroryzmu i bezpieczeństwa. Na szczeblu bardziej ogólnym Komisja i Wysoki Przedstawiciel przyjęły w dniu 7 czerwca 2017 r. wspólny komunikat „Strategiczne podejście do kwestii odporności w ramach działań zewnętrznych UE”³⁴. Celem jest wspieranie krajów partnerskich w zwiększaniu swojej odporności na globalne wyzwania w dzisiejszym świecie. W komunikacie uznano potrzebę odejścia od ograniczania skutków kryzysu w stronę bardziej ustrukturyzowanego, długoterminowego podejścia do podatności na zagrożenia, z naciskiem na przewidywanie, zapobieganie i gotowość.

Odporność na zagrożenia cybernetyczne warunkiem rozwoju

UE udziela wsparcia państwom spoza Europy w celu wzmocnienia odporności ich sieci informacyjnych. Jednym z nieodłącznych wymiarów zwiększającego się stopnia cyfryzacji jest kwestia bezpieczeństwa, rodząca szczególne wyzwania w zakresie zapewnienia odporności systemów sieci informacyjnych na całym świecie, ze względu na fakt, że dla ataków cybernetycznych granice nie mają znaczenia. UE wspiera państwa trzecie w rozwijaniu przez nie zdolności do adekwatnego zapobiegania przypadkowym awariom oraz atakom cybernetycznym i reagowania na nie. W następstwie projektu pilotażowego w dziedzinie bezpieczeństwa cybernetycznego w byłej jugosłowiańskiej republice Macedonii, Kosowie³⁵ i Mołdawii, zakończonego w 2016 r., Komisja rozpocznie realizację nowego programu w celu zwiększenia odporności państw trzecich na zagrożenia cybernetyczne – głównie państw w Afryce i Azji, ale także Ukrainy – przewidzianego na lata 2017–2020. Jego celem jest zwiększenie bezpieczeństwa i gotowości krytycznej infrastruktury informatycznej i sieci w państwach trzecich w oparciu o podejście zakładające zaangażowanie wszystkich władz, przy jednoczesnym zapewnieniu poszanowania praw człowieka i przepisów prawa.

Ochrona lotnictwa

Lotnictwo cywilne jest nadal znaczącym i symbolicznym celem ataków terrorystycznych, ale mogłoby również stać się celem w ramach kampanii hybrydowej. UE ustanowiła solidne ramy ochrony lotnictwa, mimo to loty wykonywane z państw trzecich mogą być w większym stopniu podatne na zagrożenia. Stosując się do rezolucji Rady Bezpieczeństwa ONZ nr 2309 (2016), Komisja intensyfikuje wysiłki w celu rozwoju zdolności w państwach trzecich. W styczniu 2017 r. Komisja zainicjowała nową zintegrowaną ocenę ryzyka, aby zapewnić określanie priorytetów i koordynację wysiłków w zakresie rozwijania zdolności podejmowanych na szczeblu UE i państw członkowskich, jak również we współpracy z partnerami międzynarodowymi. W 2016 r. Komisja rozpoczęła realizację 4-letniego projektu dotyczącego ochrony lotnictwa cywilnego w Afryce i na Półwyspie Arabskim w celu zwalczania zagrożenia terroryzmem w lotnictwie cywilnym. Projekt ten dotyczy głównie wymiany wiedzy fachowej między państwami partnerskimi a ekspertami z państw członkowskich należących do Europejskiej Konferencji Lotnictwa Cywilnego, a także działań w zakresie mentoringu, szkoleń i coachingu. W 2017 r. działania te zostaną zintensyfikowane.

³⁴Wspólny komunikat do Parlamentu Europejskiego i Rady: Strategiczne podejście do kwestii odporności w ramach działań zewnętrznych UE, JOIN(2017) 21 final.

³⁵ Użycie tej nazwy nie wpływa na stanowiska w sprawie statusu Kosowa i jest zgodne z rezolucją Rady Bezpieczeństwa ONZ 1244 oraz z opinią Międzynarodowego Trybunału Sprawiedliwości w sprawie Deklaracji niepodległości Kosowa

c. ZAPOBIEGANIE KRYZYSOM, REAGOWANIE NA NIE I PRZEWYCIEŻANIE ICH SKUTKÓW

Negatywne skutki można ograniczać poprzez długoterminowe strategie na szczeblu krajowym i unijnym, jednak w perspektywie krótkoterminowej konieczne jest zwiększenie zdolności państw członkowskich i Unii do zapobiegania zagrożeniom hybrydowym, reagowania na nie i przewycięzania ich skutków w sposób szybki i skoordynowany. Zasadnicze znaczenie ma szybkie reagowanie na zdarzenia spowodowane zagrożeniami hybrydowymi. W ubiegłym roku osiągnięto znaczne postępy w tym zakresie, wprowadzając stosowany obecnie w UE protokół operacyjny, w którym określono procedury zarządzania kryzysowego w przypadku ataku hybrydowego. W przyszłości monitorowanie i ćwiczenia przeprowadzane będą regularnie.

Działanie 19: Wysoki Przedstawiciel i Komisja, we współpracy z państwami członkowskimi, ustanowią wspólny protokół operacyjny i będą regularnie przeprowadzać działania w celu poprawy zdolności do podejmowania strategicznych decyzji w odpowiedzi na zagrożenia hybrydowe o złożonym charakterze, korzystając z procedur zarządzania kryzysowego i zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych.

We wspólnych ramach zalecono ustanowienie mechanizmów szybkiego reagowania na zdarzenia wywołane zagrożeniami hybrydowymi, w celu skoordynowania mechanizmów reagowania³⁶ i systemów wczesnego ostrzegania w UE. W tym celu służby Komisji i ESDZ wydały unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym (unijny podręcznik taktyczny)³⁷, w którym określono tryby koordynacji, syntezy i analizy danych wywiadowczych, dostarczania informacji na potrzeby procesów kształtowania polityki, przeprowadzania ćwiczeń i szkoleń, a także współpracy z organizacjami partnerskimi, w szczególności NATO, w razie zagrożenia hybrydowego. Również NATO opracowała podręcznik taktyczny na potrzeby ściślejszej współpracy między NATO a UE w celu zapobiegania i przeciwdziałania zagrożeniom hybrydowym w obszarach cyberobrony, komunikacji strategicznej, orientacji sytuacyjnej i zarządzania kryzysowego. Jesienią 2017 r. przeprowadzone zostanie ćwiczenie w celu przetestowania unijnego podręcznika taktycznego, będące częścią równoległego i skoordynowanego ćwiczenia Unii Europejskiej, realizowanego we współpracy z NATO.

Działanie 20: Komisja i Wysoki Przedstawiciel, w granicach swoich kompetencji, zbadają możliwość zastosowania i praktyczne skutki art. 222 TFUE i art. 42 ust. 7 TUE w razie wystąpienia poważnego ataku hybrydowego o szerokim zasięgu.

Art. 42 ust. 7 TUE dotyczy napaści zbrojnej na terytorium państwa członkowskiego, natomiast art. 222 TFUE (klauzula solidarności) dotyczy ataku terrorystycznego lub klęski żywiołowej bądź katastrofy spowodowanej przez człowieka na terytorium państwa członkowskiego. W przypadku ataków hybrydowych, które są połączeniem działań przestępczych i wywrotowych, bardziej prawdopodobne jest zastosowanie tego ostatniego artykułu. Następstwem powołania się na klauzulę solidarności jest koordynacja na szczeblu Rady (zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w

³⁶ Przyjęte przez Radę zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), stworzony przez Komisję system ARGUS oraz mechanizm reagowania w sytuacjach kryzysowych ESDZ.

³⁷ Dokument roboczy służb Komisji SWD(2016) 227, przyjęty 7 lipca 2016 r.

sytuacjach kryzysowych) oraz zaangażowanie właściwych instytucji, agencji i jednostek administracyjnych UE, a także uruchomienie unijnych programów pomocowych i mechanizmów. W decyzji Rady 2014/415/UE zawarto uzgodnienia dotyczące zastosowania przez Unię klauzuli solidarności. Te zasady stosowania nie utraciły swojej ważności, nie ma więc potrzeby dokonywania przeglądu tej decyzji Rady. Jeżeli częścią ataku hybrydowego jest napaść zbrojna, można również powołać się na art. 42 ust. 7. W takim przypadku pomocy i wsparcia powinny udzielić zarówno państwa członkowskie, jak i UE. Komisja oraz Wysoki Przedstawiciel będą kontynuować ocenę najskuteczniejszych sposobów odpierania takich ataków.

Bezpośrednim wkładem w tę ocenę jest przyjęcie wspomnianego wyżej protokołu operacyjnego UE, który zostanie przetestowany w ramach unijnego równoległego i skoordynowanego ćwiczenia (ang. *Parallel and Coordinated Exercise*, PACE) w październiku 2017 r. Podczas tego ćwiczenia przetestowane zostaną różne mechanizmy UE i jej zdolność do współdziałania w celu przyspieszenia procesu podejmowania decyzji, w przypadku gdy niejasności wywołane zagrożeniem hybrydowym utrudniają uzyskanie przejrzystego obrazu sytuacji.

Działanie 21: Wysoki Przedstawiciel, we współpracy z państwami członkowskimi, zajmie się zintegrowaniem, wykorzystaniem i koordynacją zdolności działań wojskowych w zakresie przeciwdziałania zagrożeniom hybrydowym w ramach wspólnej polityki bezpieczeństwa i obrony.

W lipcu 2017 r., w odpowiedzi na zadanie zintegrowania zdolności wojskowych w celu wsparcia WPZiB/WPBiO, a także w następstwie seminarium z udziałem ekspertów wojskowych w grudniu 2016 r. i w oparciu o wytyczne Grupy Roboczej ds. Komitetu Wojskowego Unii Europejskiej z maja 2017 r., zakończono opracowywanie opinii wojskowej w sprawie wojskowego wkładu UE w przeciwdziałanie zagrożeniom hybrydowym w ramach WPBiO, która zostanie uwzględniona w planie wdrażania rozwoju koncepcji.

d. WSPÓŁPRACA UE-NATO

Działanie 22: Wysoki Przedstawiciel, w porozumieniu z Komisją, będzie kontynuował nieformalny dialog i dążył do pogłębienia współpracy i koordynacji z NATO w zakresie orientacji sytuacyjnej, łączności strategicznej, bezpieczeństwa cybernetycznego i „zapobiegania kryzysom i reagowania na nie” w celu przeciwdziałania zagrożeniom hybrydowym zgodnie z zasadą uczestnictwa, a także zasadą autonomii procesu podejmowania decyzji każdej z tych organizacji.

Na podstawie wspólnej deklaracji podpisanej w Warszawie w dniu 8 lipca 2016 r. przez przewodniczących Rady Europejskiej i Komisji Europejskiej oraz Sekretarza Generalnego NATO, UE i NATO opracowały wspólny zestaw 42 propozycji jej realizacji, który następnie w dniu 6 grudnia 2016 r. został zatwierdzony w wyniku oddzielnych, równoległych procedur przez Rady zarówno UE, jak i NATO³⁸. W czerwcu 2017 r. Wysoki Przedstawiciel/Wiceprzewodnicząca Komisji oraz Sekretarz Generalny NATO opublikowali sprawozdanie dotyczące ogólnych postępów w realizacji 42 działań na podstawie wspólnej deklaracji. Przeciwdziałanie zagrożeniom hybrydowym jest jednym z siedmiu obszarów współpracy określonych we wspólnej deklaracji i stanowi przedmiot dziesięciu spośród czterdziestu dwóch działań. W sprawozdaniu wykazano, że wspólne wysiłki poczynione w ciągu ostatniego roku przyniosły znaczące rezultaty. Powyżej wymieniono już wiele

³⁸ <http://www.consilium.europa.eu/pl/press/press-releases/2016/12/06-eu-nato-joint-declaration/>

konkretnych działań w celu zwalczania zagrożeń hybrydowych, w tym europejskie centrum doskonałości ds. zwalczania zagrożeń hybrydowych, osiągnięcie lepszej orientacji sytuacyjnej, ustanowienie komórki UE ds. syntezy informacji o zagrożeniach hybrydowych i jej kontakty z nowo utworzonym w NATO działem ds. analizy zagrożeń hybrydowych oraz współpracę między zespołami ds. komunikacji strategicznej. Po raz pierwszy sztaby NATO i UE przeciwczą wspólnie scenariusz reakcji na atak hybrydowy. Celem tego ćwiczenia ma być przetestowanie realizacji ponad jednej trzeciej wspólnych propozycji. UE przeprowadzi w tym roku własne równoległe i skoordynowane ćwiczenie i przygotowuje się do przejęcia przewodniej roli w roku 2018.

W kwestii odporności sztaby UE i NATO rozpoczęły wzajemne briefingi, w tym na temat mechanizmu UE na rzecz zintegrowanego reagowania na szczeblu politycznym w sytuacjach kryzysowych. Regularne kontakty między sztabami UE i NATO, także w ramach warsztatów i NATO lub udziału w Radzie Sterującej Europejskiej Agencji Obrony, umożliwiły wymianę informacji na temat podstawowych wymogów NATO dotyczących krajowego poziomu odporności. Na jesień planowane są dalsze rozmowy między Komisją a NATO dotyczące wzmacniania odporności. W kolejnym sprawozdaniu z postępów we współpracy między UE a NATO zaproponowane zostaną sposoby rozszerzenia współpracy między tymi dwiema organizacjami.

3. WNIOSKI

We wspólnych ramach przedstawiono działania, które mają pomóc w przeciwdziałaniu zagrożeniom hybrydowym i zwiększyć odporność na szczeblu UE i państw członkowskich, a także partnerów. Komisja i Wysoki Przedstawiciel, w ścisłej współpracy z państwami członkowskimi i partnerami, pomyślnie realizują działania we wszystkich obszarach, kluczowe jest jednak utrzymanie obecnej dynamiki w obliczu rozwijających się i ulegających ciągłym przeobrażeniom zagrożeń hybrydowych. Odpowiedzialność za przeciwdziałanie zagrożeniom hybrydowym związanym z bezpieczeństwem narodowym i utrzymaniem porządku publicznego spoczywa w pierwszej kolejności na państwach członkowskich. Zwiększanie odporności krajowej i zbiorowe wysiłki na rzecz ochrony przed zagrożeniami hybrydowymi należy pojmować jako wzajemnie wspierające się elementy tego samego kompleksowego wysiłku. Zachęca się zatem państwa członkowskie do jak najszybszego przeprowadzenia badań na temat zagrożeń hybrydowych, gdyż dostarczą one cennych informacji na temat stopnia podatności na zagrożenia i gotowości w całej Europie. Biorąc pod uwagę znaczne postępy poczynione w poprawie orientacji sytuacyjnej, należy zwiększyć do maksimum potencjał komórki UE ds. syntezy informacji. Wysoki Przedstawiciel wzywa państwa członkowskie do wspierania prac grup zadaniowych ds. komunikacji strategicznej, aby skuteczniej przeciwdziałać wzrastającym zagrożeniom hybrydowym. UE będzie udzielać pełnego wsparcia utworzonemu przez Finlandię Europejskiemu Centrum ds. Zwalczania Zagrożeń Hybrydowych.

Wyjątkowym atutem UE jest wsparcie, jakiego udziela państwom członkowskim i partnerom w zwiększaniu ich odporności, z wykorzystaniem szerokiego wachlarza istniejących instrumentów i programów. Odnotowano znaczne postępy w działaniach w celu zwiększania odporności w dziedzinach takich jak transport, energia, bezpieczeństwo cybernetyczne, infrastruktura krytyczna, ochrona systemu finansowego przed nielegalnym wykorzystaniem i wysiłki na rzecz przeciwdziałania brutalnemu ekstremizmowi i radykalizacji postaw. UE będzie kontynuować działania w celu zwiększania odporności w obliczu zmieniającego się charakteru zagrożeń hybrydowych. W szczególności UE opracuje wskaźniki służące

poprawie ochrony i odporności infrastruktury krytycznej na wypadek zagrożeń hybrydowych w istotnych sektorach.

Ze środków Europejskiego Funduszu Obrony współfinansowane mogą być, z udziałem państw członkowskich, priorytetowe działania w zakresie zdolności, umożliwiające zwiększenie odporności na zagrożenia hybrydowe. W szczególności pakiet dotyczący bezpieczeństwa cybernetycznego, który ma zostać wkrótce przyjęty, jak również środki międzysektorowe służące wdrożeniu dyrektywy w sprawie bezpieczeństwa sieci i informacji zaowocują stworzeniem nowych platform ds. przeciwdziałania zagrożeniom hybrydowym w całej UE.

Komisja oraz Wysoki Przedstawiciel wzywają państwa członkowskie i zainteresowane strony, w stosownych przypadkach, do szybkiego osiągnięcia porozumienia i zapewnienia szybkiego i skutecznego wdrożenia licznych środków służących wzmocnieniu odporności, wspomnianych w niniejszym komunikacie. UE będzie polegać w swoich działaniach na owocnej dotychczas współpracy z NATO i będzie ją pogłębiać.

Unia podtrzymuje swoje zobowiązanie do mobilizacji wszystkich stosownych instrumentów unijnych w celu zwalczania złożonych zagrożeń hybrydowych. Wspieranie wysiłków państw członkowskich jest nadal kwestią priorytetową dla Unii, występującej w charakterze silniejszego i skuteczniej reagującego gwaranta bezpieczeństwa, wspólnie ze swoimi głównymi partnerami.