KOMISJA
EUROPEJSKA

WYSOKI PRZEDSTAWICIEL UNII
DO SPRAW ZAGRANICZNYCH I
POLITYKI BEZPIECZEŃSTWA

Bruksela, dnia 6.4.2016 r.
JOIN(2016) 18 final

WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY

Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym

odpowiedź Unii Europejskiej

1. WPROWADZENIE

W ostatnich latach zaszły radykalne zmiany w środowisku bezpieczeństwa Unii Europejskiej. Kluczowe zagrożenia dla pokoju i stabilności we wschodnim i południowym sąsiedztwie UE nadal wskazują na konieczność dostosowania i wzmocnienia przez Unię swoich zdolności jako gwaranta bezpieczeństwa i skoncentrowania się na ścisłej współzależności między bezpieczeństwem zewnętrznym i wewnętrznym. Przyczyną wielu obecnych wyzwań w zakresie pokoju, bezpieczeństwa i dobrobytu jest niestabilność w najbliższym sąsiedztwie UE i ewoluujące formy zagrożeń. Przewodniczący Komisji Europejskiej Jean-Claude Juncker podkreślił w swoich wytycznych politycznych z 2014 r. potrzebę dążenia do silniejszej Europy pod względem bezpieczeństwa i obrony, a także łączenia instrumentów unijnych i krajowych w bardziej skuteczny sposób niż miało to miejsce w przeszłości. W reakcji na zaproszenie od Rady do Spraw Zagranicznych z dnia 18 maja 2015 r. Wysoki Przedstawiciel w ścisłej współpracy ze służbami Komisji i Europejską Agencją Obrony, a także w porozumieniu z państwami członkowskimi UE zobowiązał się przedstawić niniejsze wspólne ramy wraz z wykonalnymi propozycjami, tak by pomóc przeciwdziałać zagrożeniom hybrydowym i budować odporność UE i państw członkowskich, a także partnerów[1]. W czerwcu 2015 r. Rada Europejska odwołała konieczność mobilizacji instrumentów UE mających pomóc przeciwdziałać zagrożeniom hybrydowym[2].

Mimo że zagrożenia hybrydowe są różnie definiowane i definicje te należy formułować w sposób elastyczny, tak by uwzględniały one zmienny charakter tego rodzaju zagrożeń, pojęcie to oznacza kombinację represyjnych i wywrotowych działań, konwencjonalnych i niekonwencjonalnych metod (tj. dyplomatycznych, militarnych, ekonomicznych i technologicznych), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe, by osiągnąć określone cele, przy czym działania te są poniżej progu oficjalnie wypowiedzianej wojny. Zazwyczaj nacisk kładzie się na wykorzystanie podatności danego celu na zagrożenia i kreowanie dwuznaczności, by utrudnić procesy decyzyjne. Kampanie dezinformacyjne prowadzone na masową skalę przy wykorzystaniu mediów społecznościowych w celu kontrolowania dyskursu politycznego lub radykalizowania postaw, rekrutacji „grup-przykrywek" i kierowania nimi mogą być nośnikiem zagrożeń hybrydowych.

W zakresie, w jakim przeciwdziałanie zagrożeniom hybrydowym dotyczy bezpieczeństwa narodowego, obrony narodowej i utrzymania porządku publicznego, główna odpowiedzialność spoczywa na państwach członkowskich, gdyż większość podatności na zagrożenia jest specyficznych dla danego państwa. Wiele państw członkowskich UE stoi jednak w obliczu wspólnych zagrożeń, które mogą również być skierowane przeciwko transgranicznym sieciom lub infrastrukturze. Takie zagrożenia można skuteczniej eliminować w drodze skoordynowanej reakcji na poziomie UE, stosując strategie i instrumenty UE, by móc czerpać z poczucia solidarności w Europie,

[1] Konkluzje Rady w sprawie wspólnej polityki bezpieczeństwa i obrony (WPBiO), maj 2015 r. [Consilium 8971/15]
[2] Konkluzje Rady Europejskiej, czerwiec 2015 r. [EUCO 22/15].

wzajemnej pomocy i wszelkich możliwości, jakie niesie z sobą traktat lizboński. Strategie i instrumenty UE mogą odgrywać – i w znacznym stopniu już odgrywają – istotną rolę i wnoszą wartość dodaną w szerzeniu wiedzy. Jest to pomocne w budowaniu większej odporności państw członkowskich na wspólne zagrożenia. Zewnętrzne działania Unii, które są przewidziane w niniejszych ramach, realizowane są zgodnie z zasadami określonymi w art. 21 Traktatu o Unii Europejskiej (TUE), tj. zasadą demokracji, praworządności, uniwersalności i niepodzielności praw człowieka i poszanowaniem zasad Karty Narodów Zjednoczonych i prawa międzynarodowego[3].

Niniejszy wspólny komunikat ma ułatwić stosowanie kompleksowego podejścia, co umożliwi UE, w koordynacji z państwami członkowskimi, przeciwdziałanie w szczególności zagrożeniom hybrydowym poprzez osiągnięcie synergii między wszystkimi istotnymi instrumentami i zacieśnianie współpracy między wszystkimi odnośnymi podmiotami[4]. Działania opierają się na istniejących strategiach i politykach sektorowych, które przyczyniają się do zwiększenia bezpieczeństwa. W szczególności pomocne w zwalczaniu zagrożeń hybrydowych mogą być Europejska agenda bezpieczeństwa[5], planowana globalna strategia UE w dziedzinie polityki zagranicznej i bezpieczeństwa i europejski plan działań w sektorze obrony[6], strategia Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego,[7] europejska strategia bezpieczeństwa energetycznego,[8] strategia Unii Europejskiej w zakresie bezpieczeństwa morskiego[9].

W związku z tym, że obecnie NATO również angażuje się w zwalczanie zagrożeń hybrydowych, a Rada do Spraw Zagranicznych zaproponowała pogłębioną współpracę i koordynację w tym obszarze, niektóre z wniosków mają na celu usprawnienie współpracy między UE i NATO w dziedzinie zwalczania zagrożeń hybrydowych.

Zaproponowane działanie koncentruje się na następujących elementach: podnoszeniu świadomości, budowaniu odporności, przeciwdziałaniu kryzysowi, reagowaniu na sytuacje kryzysowe i przezwyciężaniu skutków kryzysu.

2. ROZPOZNANIE HYBRYDOWEGO CHARAKTERU ZAGROŻENIA

Zagrożenia hybrydowe mają na celu wykorzystanie podatności na zagrożenia danego państwa i nierzadko podważenie podstawowych wartości i swobód demokratycznych. Pierwszym krokiem będzie współpraca między Wysokim Przedstawicielem i Komisją z państwami członkowskimi na rzecz lepszej orientacji sytuacyjnej poprzez monitorowanie

[3] Karta praw podstawowych Unii Europejskiej jest wiążąca dla instytucji i państw członkowskich, gdy wdrażają one prawo unijne.
[4] Ewentualne wnioski ustawodawcze będą podlegać wymogom lepszego stanowienia prawa przez Komisję zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa, SWD(2015) 111.
[5] COM(2015) 185 final.
[6] Strategia ma zostać przedstawiona w 2016 r.
[7] Ramy polityki UE w zakresie cyberobrony [Consilium 15585/14] i wspólny komunikat „Strategia Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego: otwarta, bezpieczna i chroniona cyberprzestrzeń", luty 2013 r. [JOIN(2013)1].
[8] Wspólny komunikat „Europejska strategia bezpieczeństwa energetycznego", maj 2014 r. [SWD(2014) 330].
[9] Wspólny komunikat „Otwarty i bezpieczny światowy obszar morski: elementy strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego" — JOIN(2014) 9 final — 6.3.2014 r.

i ocenę zagrożeń, które mogą być wymierzone w słabe punkty UE. Komisja opracowuje metody oceny ryzyka dla bezpieczeństwa, które mają pomóc w informowaniu decydentów i promowaniu podejścia opartego na ocenie ryzyka w obszarach takich jak ochrona lotnictwa, finansowanie terroryzmu i pranie pieniędzy. Ponadto konieczne byłoby badanie przeprowadzone przez państwa członkowskie mające na celu zidentyfikowanie obszarów podatnych na zagrożenia hybrydowe. Celem byłoby określenie wskaźników dotyczących zagrożeń hybrydowych, uwzględnienie ich w mechanizmach wczesnego ostrzegania i oceny ryzyka oraz w miarę potrzeby ich rozpowszechnianie.

<u>Działanie 1</u>: 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.

3. ODPOWIEDŹ UE NA ZAGROŻENIA - ORGANIZOWANIE DZIAŁAŃ: PODNOSZENIE ŚWIADOMOŚCI

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

Istotne znaczenie ma, by UE we współpracy z państwami członkowskimi miała odpowiedni poziom orientacji sytuacyjnej, by móc dostrzegać wszelkie zmiany w środowisku bezpieczeństwa mające związek z działaniami hybrydowymi wywołane przez podmioty państwowe lub niepaństwowe. By móc skutecznie przeciwdziałać zagrożeniom hybrydowym, ważne jest usprawnienie wymiany informacji i propagowanie wymiany odnośnych informacji wywiadowczych w sektorach i między Unią Europejską, jej państwami członkowskimi i partnerami.

Komórka UE ds. syntezy informacji będzie zajmować się wyłącznie analizą zagrożeń hybrydowych i działać przy Centrum Analiz Wywiadowczych Unii Europejskiej powołanym przy Europejskiej Służbie Działań Zewnętrznych (ESDZ). Komórka ta otrzymywałaby do analizy i publikacji informacje niejawne, a także informacje ze źródeł jawnych, w szczególności na temat wskaźników i ostrzeżeń dotyczących zagrożeń hybrydowych od różnych zainteresowanych podmiotów w ESDZ (w tym delegatur Unii), Komisji (wraz z agencjami UE[10]) i państwach członkowskich. Ponadto we współpracy z podobnymi organami działającymi na szczeblu UE[11] i państw członkowskich, komórka UE ds. syntezy informacji analizowałaby zewnętrzne aspekty zagrożeń hybrydowych wpływających na sytuację w UE i jej sąsiedztwie, by móc szybko analizować odnośne incydenty i zapewniać informacje niezbędne dla procesów podejmowania strategicznych decyzji w UE, w tym przez zapewnianie wkładu w oceny ryzyka w odniesieniu do

[10] Zgodnie z ich pełnomocnictwami.

[11] Na przykład działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością i Europejskie Centrum ds. Zwalczania Terroryzmu, Frontex, unijny zespół reagowania na incydenty komputerowe (CERT)-EU).

bezpieczeństwa dokonywane na poziomie UE. Wyniki analiz dokonywanych przez komórkę UE ds. syntezy informacji byłyby przetwarzane i wykorzystywane zgodnie z unijnymi przepisami dotyczącymi ochrony informacji i danych niejawnych[12]. Komórka powinna współpracować z organami działającymi na szczeblu UE i państw członkowskich. Państwa członkowskie powinny powołać krajowy punkt kontaktowy, który będzie powiązany z komórką UE ds. syntezy informacji. Personel UE zatrudniony poza terenem Unii (w tym pracownicy delegatur Unii, personel oddelegowany na misje i operacje UE) i w państwach członkowskich powinien również przejść szkolenia z rozpoznawania wczesnych sygnałów zagrożeń hybrydowych.

***Działanie 2*: Powołanie komórki UE ds. syntezy informacji w ramach struktury Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN), 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.**

3.2. Komunikacja strategiczna

Sprawcy zagrożeń hybrydowych mogą systematycznie rozpowszechniać nieprawdziwe informacje, wykorzystując w tym celu media społecznościowe, dążąc tym samym do zradykalizowania postaw, zdestabilizowania społeczeństwa i przejęcia kontroli nad dyskursem politycznym. Ogromne znaczenie ma zdolność reagowania na zagrożenia hybrydowe przy wykorzystaniu dobrze opracowanej **komunikacji strategicznej**. Do głównych czynników budowania odporności społeczeństwa należy udzielanie szybkich i faktycznych odpowiedzi oraz podnoszenie wiedzy społeczeństwa na temat zagrożeń hybrydowych.

Komunikacja strategiczna powinna w pełni wykorzystywać do tego celu m.in. media społecznościowe, a także tradycyjne media wizualne, audio i internetowe. ESDZ, korzystając z działalności grup zadaniowych *East and Arab Stratcom Task Forces*, powinna zoptymalizować wykorzystanie lingwistów z płynną znajomością odnośnych języków niebędących językami UE i specjalistów od mediów społecznościowych, którzy mogą monitorować informacje poza UE i zapewniać ukierunkowaną komunikację w celu reagowania na dezinformacje. Ponadto państwa członkowskie powinny opracować skoordynowane mechanizmy komunikacji strategicznej w celu wspierania procesu wskazywania źródeł i przeciwdziałania szerzeniu dezinformacji, by ujawniać zagrożenia hybrydowe.

***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.**

[12] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

3.3. Centrum doskonałości „przeciwdziałające zagrożeniom hybrydowym""

Korzystając z doświadczenia niektórych państw członkowskich i organizacji partnerskich[13], instytucja wielonarodowa lub sieć takich instytucji mogłaby działać w charakterze centrum doskonałości ds. eliminowania zagrożeń hybrydowych. Takie centrum mogłoby skoncentrować się na badaniu, w jaki sposób stosowane są strategie hybrydowe, a także mogłoby sprzyjać rozwojowi nowych koncepcji i technologii w sektorze prywatnym i przemyśle, by pomóc państwom członkowskim budować odporność. Badania te mogłyby przyczynić się do zbliżenia polityk, doktryn i koncepcji UE i poszczególnych państw członkowskich oraz pomóc dopilnować, by w procesie podejmowania decyzji można było uwzględniać stopień złożoności zagrożeń hybrydowych i związane z nimi niejasności. Wspomniane centrum powinno opracowywać programy w celu nadania tempa badaniom i zadaniom, tym samym znalezienia praktycznych rozwiązań istniejących problemów, jakie wynikają z zagrożeń hybrydowych. Mocną stroną takiego centrum byłaby wiedza fachowa wniesiona przez wielonarodowy i przekrojowy zespół uczestników z sektora cywilnego i wojskowego, prywatnego i akademickiego.

Takie centrum mogłoby ściśle współpracować z istniejącymi centrami doskonałości działającymi przy UE[14] i NATO[15], by korzystać z wiedzy na temat zagrożeń hybrydowych zebranej w dziedzinie cyberobrony, komunikacji strategicznej, współpracy cywilno-wojskowej, działań w zakresie energii i reagowania w sytuacjach kryzysowych.

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

4. ODPOWIEDŹ UE NA ZAGROŻENIA - ORGANIZOWANIE DZIAŁAŃ: BUDOWANIE ODPORNOŚCI

Odporność oznacza zdolność do znoszenia stresu, odzyskiwania sił i powrotu do mocniejszej formy po zwalczeniu problemów. By skutecznie zwalczać zagrożenia hybrydowe, należy wyeliminować potencjalne podatności w kluczowej infrastrukturze, łańcuchach dostaw i społeczeństwie. Można poprawić odporność infrastruktury na poziomie UE, korzystając z instrumentów i polityk UE.

4.1. Ochrona infrastruktury krytycznej

Istotne znaczenie ma ochrona infrastruktury krytycznej (np. łańcuch dostaw energii, transport), gdyż niekonwencjonalny atak sprawców zagrożeń hybrydowych na „miękkie cele" mógłby doprowadzić do poważnych zakłóceń w gospodarce i społeczeństwie. By zapewnić ochronę infrastruktury krytycznej, europejski program ochrony infrastruktury

[13] Centra doskonałości NATO.
[14] Np. Instytut Unii Europejskiej Studiów nad Bezpieczeństwem, tematyczne centra doskonałości UE zajmujące się zagrożeniami chemicznymi, biologicznymi, radiologicznymi i jądrowymi (CBRN).
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm

krytycznej[16] zapewnia podejście systemowe obejmujące wszystkie rodzaje ryzyka, wszystkie sektory i uwzględniające współzależności, na podstawie wdrożenia działań w zakresie zapobiegania, gotowości i reagowania. Dyrektywa w sprawie europejskiej infrastruktury krytycznej[17] ustanawia procedurę rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej i wspólne podejście do oceny potrzeb w zakresie poprawy jej ochrony. W szczególności należy wznowić prace w ramach wspomnianej dyrektywy nad wzmocnieniem odporności infrastruktury krytycznej dotyczącej transportu (np. główne porty lotnicze i porty handlowe UE). Komisja oceni, czy należy opracować wspólne narzędzia, m.in. wskaźniki, w celu wzmocnienia odporności infrastruktury krytycznej na zagrożenia hybrydowe we wszystkich istotnych sektorach.

<u>Działanie 5</u>: 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.

4.1.1. Sieci energetyczne

Niezakłócona produkcja i dystrybucja energii ma ogromne znaczenie dla UE, a istotne awarie zasilania mogłyby przynieść szkody. Zasadniczym środkiem w obszarze przeciwdziałania zagrożeniom hybrydowym jest dalsza dywersyfikacja unijnych źródeł energii, dostawców i tras dostaw, by zapewnić bezpieczniejsze i bardziej odporne dostawy energii. Komisja prowadzi obecnie również oceny ryzyka i bezpieczeństwa (testy wytrzymałościowe) w elektrowniach w UE. By zapewnić dywersyfikację, prowadzone są intensywne prace w ramach strategii na rzecz unii energetycznej: na przykład, południowy korytarz gazowy może zapewnić dostawy gazu z rejonu Morza Kaspijskiego do Europy, a w Europie Północnej tworzone są centra handlu gazem skroplonym (tzw. huby) z wieloma dostawcami. Za podanym przykładem powinny pójść państwa w Europie Środkowo-Wschodniej i w rejonie Morza Śródziemnego, gdzie w budowie znajduje się centrum handlu gazem[18]. Rozwijający się rynek zbytu skroplonego gazu ziemnego pomoże również w osiąganiu tego celu.

Jeśli chodzi o materiały i obiekty jądrowe, Komisja wspiera rozwój i stosowanie najwyższych norm bezpieczeństwa, tym samym wzmacniając odporność. Komisja zachęca do konsekwentnej transpozycji do prawa krajowego i wdrożenia dyrektywy w sprawie bezpieczeństwa jądrowego[19] określającej zasady zapobiegania wypadkom i łagodzenia skutków wypadków, a także przepisów dyrektywy ustanawiającej

[16] Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej. 12.12.2006 r., COM(2006) 786 final.
[17] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz.U. L 345 z 23.12.2008.
[18] O dotychczasowych postępach można dowiedzieć się z komunikatu Komisji „Stan unii energetycznej w 2015 r." (COM(2015) 572 final.
[19] Dyrektywa Rady 2009/71/Euratom z dnia 25 czerwca 2009 r. ustanawiająca wspólnotowe ramy bezpieczeństwa jądrowego obiektów jądrowych, zmieniona dyrektywą Rady 2014/87/Euratom z dnia 8 lipca 2014 r.

podstawowe normy bezpieczeństwa[20] dotyczących międzynarodowej współpracy w zakresie gotowości na sytuacje awaryjne i reagowania na nie, w szczególności między sąsiadującymi państwami członkowskimi i z państwami sąsiadującymi.

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.

4.1.2. Bezpieczeństwo transportu i łańcucha dostaw

Transport ma zasadnicze znaczenie dla funkcjonowania Unii. Ataki hybrydowe na infrastrukturę transportową (taką jak porty lotnicze, infrastruktura drogowa, porty i drogi kolejowe) mają poważne konsekwencje i prowadzą do zakłóceń w podróżowaniu i łańcuchach dostaw. Przy wdrażaniu przepisów prawnych dotyczących bezpieczeństwa lotniczego i morskiego[21] Komisja dokonuje regularnych inspekcji[22], a działając na rzecz bezpieczeństwa transportu lądowego, zmierza do wyeliminowania pojawiających się zagrożeń hybrydowych. W tym kontekście omawiane są ramy UE w świetle zmienionego rozporządzenia w sprawie bezpieczeństwa lotniczego[23] będącego częścią europejskiej strategii w dziedzinie lotnictwa[24]. Ponadto zagrożenia dla bezpieczeństwa morskiego stanowią przedmiot strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i jej planu działania w tym zakresie[25]. Plan ten umożliwia UE i państwom członkowskim kompleksowe podejście do problemów bezpieczeństwa morskiego, w tym przeciwdziałanie zagrożeniom hybrydowym, w drodze międzysektorowej współpracy między podmiotami cywilnymi i wojskowymi, by chronić krytyczną infrastrukturę morską, globalne łańcuchy dostaw, handel morski, naturalne zasoby morskie i zasoby energetyczne. Bezpieczeństwo międzynarodowego łańcucha dostaw jest także

[20] Dyrektywa Rady 2013/59/Euratom z dnia 5 grudnia 2013 r. ustanawiająca podstawowe normy bezpieczeństwa w celu ochrony przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego oraz uchylająca dyrektywy 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom i 2003/122/Euratom.

[21] Rozporządzenie (WE) nr 300/2008 Parlamentu Europejskiego i Rady z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002; rozporządzenie wykonawcze Komisji (UE) nr 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego; dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów; rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie wzmocnienia ochrony statków i obiektów portowych;

[22] W świetle prawa UE Komisja jest zobowiązana do przeprowadzania inspekcji w celu zapewnienia prawidłowego wdrożenia wymogów w zakresie bezpieczeństwa lotniczego i morskiego przez państwa członkowskie. Są to m.in. inspekcje właściwego organu w danym państwie członkowskim, jak również kontrole na lotniskach, w portach, na statkach, u przewoźników lotniczych i w podmiotach wdrażających środki ochrony. Inspekcje Komisji mają na celu dopilnowanie, aby normy UE były w pełni wdrożone przez państwa członkowskie.

[23] Rozporządzenie Komisji (UE) 2016/4 z dnia 5 stycznia 2016 r. zmieniające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 w odniesieniu do zasadniczych wymagań w zakresie ochrony środowiska; rozporządzenie (WE) nr 216/2008 z dnia 20 lutego 2008 r. w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Transportu Lotniczego.

[24] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów: Europejska strategia w dziedzinie lotnictwa, COM/2015/0598 final z 7.12.2015 r.

[25] W grudniu 2014 r. Rada przyjęła plan działania w celu wdrożenia strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

przedmiotem strategii Unii Europejskiej dotyczącej zarządzania ryzykiem celnym i związanego z tym planu działania[26].

<u>Działanie 7</u>: 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 związanego z tym planu działania Komisja i Wysoki Przedstawiciel (w ramach swoich kompetencji), w koordynacji z państwami członkowskimi, zbadają, w jaki sposób należy odpowiedzieć na złożone zagrożenia hybrydowe, zwłaszcza te dotyczące krytycznej infrastruktury transportowej.

4.1.3 Przestrzeń kosmiczna

Zagrożenia hybrydowe mogą być skierowane przeciwko infrastrukturze kosmicznej, a ich konsekwencje mogą rzutować na sytuację w wielu sektorach. UE opracowała ramy wsparcia obserwacji i śledzenia obiektów kosmicznych[27] mające połączyć w ramach sieci tego rodzaju aktywa należące do państw członkowskich, by świadczyć usługi obserwacji i śledzenia obiektów kosmicznych[28] zidentyfikowanym użytkownikom (państwom członkowskim, instytucjom UE, właścicielom i operatorom statków kosmicznych, a także organom odpowiedzialnym za ochronę cywilną). W ramach zapowiadanej strategii kosmicznej dla Europy Komisja zbada, czy możliwy jest jej dalszy rozwój, tak by móc monitorować zagrożenia hybrydowe dla infrastruktury kosmicznej.

Łączność satelitarna (SatComs) obejmuje aktywa o kluczowym znaczeniu dla zarządzania kryzysami, reagowania w przypadku katastrof, dozoru policji, nadzoru granic i strefy przybrzeżnej. Aktywa te stanowią trzon wielkoskalowej infrastruktury, takiej jak infrastruktura transportowa, systemy statków kosmicznych lub zdalnie kierowane bezzałogowe systemy powietrzne. Zgodnie z apelem Rady Europejskiej, by przygotować nową generację rządowej łączności satelitarnej (GOVSATCOM), Komisja we współpracy z Europejską Agencją Obrony ocenia obecnie, w jaki sposób można łączyć popyt w kontekście zapowiadanej Strategii kosmicznej dla Europy i europejskiego planu działań w sektorze obrony.

W wielu przypadkach infrastruktura krytyczna funkcjonuje m.in. na podstawie informacji o dokładnym czasie, które pozwalają zsynchronizować jej sieci (np. sieci energetyczne i telekomunikacyjne) lub na podstawie transakcji dotyczących znacznika czasu (np. rynki finansowe). Zależność od globalnego systemu nawigacji satelitarnej pojedynczego sygnału synchronizacji czasu nie oferuje odporności niezbędnej do przeciwdziałania

[26] Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego dotyczący strategii UE i planu działania w zakresie zarządzania ryzykiem celnym: Przeciwdziałanie ryzyku, poprawa bezpieczeństwa łańcucha dostaw i ułatwienie wymiany handlowej, COM(2014) 527 final.

[27] Zob. decyzja 541/2014 Parlamentu Europejskiego i Rady.

[28] Takie jak ostrzeżenia o unikaniu kolizji na orbicie, alerty dotyczące destrukcji lub kolizji i ryzykownych przypadków ponownego wejścia obiektów kosmicznych do atmosfery ziemskiej.

zagrożeniom hybrydowym. Galileo, europejski system nawigacji satelitarnej, stanowiłby drugie wiarygodne źródło czasu.

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

4.2. Zdolności obronne

By wzmocnić odporność UE na zagrożenia hybrydowe, należy zwiększyć zdolności obronne. Ważne jest rozpoznanie związanych z tym kluczowych zdolności, np. w dziedzinie nadzoru i zwiadu. Europejska Agencja Obrony mogłaby pełnić rolę katalizatora rozwoju zdolności wojskowych związanych z zagrożeniami hybrydowymi (np. przez skrócenie cykli rozwoju zdolności obronnych, inwestowanie w technologie, systemy i prototypy, otwarcie biznesu obronnego na innowacyjne technologie o komercyjnym wykorzystaniu). W ramach zapowiadanego europejskiego planu działania w sektorze obrony można przeanalizować ewentualne działania.

<u>Działanie 9:</u> Wysoki Przedstawiciel, przy wsparciu – w stosownych przypadkach – ze strony państw członkowskich, we współpracy z Komisją, zaproponuje 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.

4.3. Ochrona zdrowia publicznego i bezpieczeństwo żywnościowe

Zdrowie człowieka może być zagrożone w wyniku manipulowania chorobami zakaźnymi lub zatrucia żywności, gleby, powietrza i wody pitnej przy użyciu środków chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ). Ponadto celowe rozprzestrzenianie chorób zwierząt lub roślin może mieć poważny wpływ na bezpieczeństwo żywnościowe w Unii i poważne skutki gospodarcze i społeczne dla kluczowych obszarów unijnego łańcucha żywnościowego. Na zagrożenia hybrydowe można reagować, korzystając z obecnych struktur unijnych dotyczących bezpieczeństwa zdrowotnego, ochrony środowiska i bezpieczeństwa żywności.

W świetle przepisów UE dotyczących transgranicznych zagrożeń dla zdrowia[29] istniejące mechanizmy pozwalają na utrzymanie stanu gotowości na poważne transgraniczne

[29] Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE, Dz.U. L 293 z 5.11.2013, s.1).

zagrożenia dla zdrowia, ponieważ państwa członkowskie, agencje i komitety naukowe UE[30] są zrzeszone w systemie wczesnego ostrzegania i reagowania. Komitet ds. Bezpieczeństwa Zdrowia, który odpowiada za koordynowanie planów reagowania państw członkowskich na zagrożenia, może działać jako punkt koordynacji w zakresie podatności na zagrożenia dla zdrowia publicznego[31]i zawierać kwestie związane z zagrożeniami hybrydowymi (zwłaszcza zagrożeniem bioterroryzmem) w wytycznych dotyczących komunikacji w sytuacjach kryzysowych i w działaniach państw członkowskich zmierzających do budowania zdolności (symulacja sytuacji kryzysowych). W obszarze bezpieczeństwa żywności, za pośrednictwem systemu wczesnego ostrzegania o niebezpiecznej żywności i paszach (RASFF) i wspólnego systemu zarządzania ryzykiem dla organów celnych, właściwe organy wymieniają się informacjami na temat analizy ryzyka w celu monitorowania zagrożeń dla zdrowia, jakie niesie z sobą zatruta żywność. Jeśli chodzi o zdrowie zwierząt i roślin, w wyniku przeglądu ram prawnych UE[32] do istniejącego „zestawu narzędzi" [33] dodane zostaną nowe elementy, by być lepiej przygotowanym na zagrożenia hybrydowe.

<u>Działanie 10</u>: 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.

4.4. Bezpieczeństwo cybernetyczne

UE w ogromnym stopniu korzysta z faktu, że społeczeństwo jest zdigitalizowane i wzajemnie połączone. Ataki cybernetyczne mogą zakłócać świadczenie usług cyfrowych na terenie UE i mogą być wykorzystywane przez sprawców zagrożeń hybrydowych. Wzmocnienie odporności systemów komunikacyjnych i informatycznych w Europie jest ważne dla wspierania jednolitego rynku cyfrowego. Strategia UE w zakresie bezpieczeństwa cybernetycznego i Europejska agenda bezpieczeństwa zapewniają ogólne ramy strategiczne dla inicjatyw UE w dziedzinie bezpieczeństwa cybernetycznego i cyberprzestępczości. UE angażuje się w pogłębianie wiedzy, rozwój mechanizmów współpracy i opracowywanie odpowiedzi w ramach wyników strategii bezpieczeństwa cyberprzestrzeni. W szczególności w proponowanej dyrektywie w sprawie bezpieczeństwa sieci i informacji[34] podniesiono kwestie ryzyka związanego z

[30] Decyzja Komisji C(2015) 5383 z dnia 7 sierpnia 2015 r. w sprawie utworzenia komitetów naukowych w dziedzinie zdrowia publicznego, bezpieczeństwa konsumentów i środowiska.

[31] Zgodnie z decyzją Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylającą decyzję nr 2119/98/WE, Dz.U. L 293, s. 1.

[32] Rozporządzenie 2016/429 Parlamentu Europejskiego i Rady w sprawie przenośnych chorób zwierząt oraz zmieniające i uchylające niektóre akty w dziedzinie zdrowia zwierząt („Prawo o zdrowiu zwierząt"), Dz.U. L 84 z 31.3.2016. Jeśli chodzi o rozporządzenie Parlamentu Europejskiego i Rady w sprawie środków ochronnych przeciwko agrofagom roślin („rozporządzenie w sprawie zdrowia roślin") –Parlament Europejski i Rada osiągnęły porozumienie polityczne w sprawie brzmienia rozporządzenia w dniu 16 grudnia 2015 r.

[33] Np. unijne banki szczepionek, zaawansowane elektroniczne systemy informacji na temat chorób zwierząt, większy obowiązek pomiarów po stronie laboratoriów i innych podmiotów mających do czynienia z patogenami.

[34] Wniosek Komisji dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

bezpieczeństwem cybernetycznym w odniesieniu do szerokiej grupy dostawców istotnych usług w dziedzinie energii, transportu, finansów i zdrowia. Wspomniani dostawcy, jak również dostawcy kluczowych usług cyfrowych (np. przetwarzanie w chmurze) powinni podejmować stosowne środki bezpieczeństwa i zgłaszać organom krajowym poważne incydenty, zwracając uwagę na wszelkie cechy charakterystyczne dla zagrożeń hybrydowych. Po przyjęciu wspomnianej dyrektywy przez współustawodawców jej skuteczna transpozycja do prawa krajowego i wdrożenie poprawiłyby zdolności w dziedzinie bezpieczeństwa cybernetycznego państw członkowskich, pogłębiając tym samym ich współpracę w zakresie bezpieczeństwa cyberprzestrzeni poprzez wymianę informacji i najlepszych praktyk w dziedzinie przeciwdziałania zagrożeniom hybrydowym. W szczególności dyrektywa przewiduje utworzenie sieci 28 krajowych Zespołów Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT) i CERT-UE[35] w celu realizowania dobrowolnej współpracy operacyjnej.

By zachęcić do współpracy publiczno-prywatnej i stosowania ogólnounijnego podejścia do bezpieczeństwa cybernetycznego, Komisja utworzyła platformę bezpieczeństwa sieci i informacji (NIS), która wydaje wytyczne w sprawie najlepszych praktyk dotyczących zarządzania ryzykiem. Choć państwa członkowskie ustalają wymogi i tryby bezpieczeństwa w celu zgłaszania krajowych incydentów, Komisja zachęca do znacznej konwergencji strategii w zakresie zarządzania ryzykiem, odwołując się w szczególności do Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).

<u>Działanie 11</u>: Komisja zachęca państwa członkowskie do utworzenia – w trybie priorytetowym – i pełnego wykorzystania sieci 28 zespołów CSIRT i CERT-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 NIS, takimi jak zdolność do gromadzenia informacji, łączenia wiedzy fachowej i szybkich reakcji.

4.4.1. Przemysł

Coraz większe poleganie na przetwarzaniu w chmurze i dużych zbiorach danych zwiększa podatność na zagrożenia hybrydowe. Strategia jednolitego rynku cyfrowego przewiduje umowne partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego [36], które skoncentruje się na badaniach naukowych i innowacjach, a także pomoże Unii utrzymać wysoki stopień zdolności technologicznych w tym obszarze. Umowne partnerstwo publiczno-prywatne zbuduje zaufanie między różnymi graczami na rynku i stworzy synergię między popytem i podażą. Mimo że takie umowne partnerstwo publiczno-prywatne i środki wspierające będą przede wszystkim skoncentrowane na produktach dotyczących cywilnego bezpieczeństwa cybernetycznego

COM(2013) 48 final z 7.2.2013 r. Rada Unii Europejskiej i Parlament Europejski osiągnęły porozumienie polityczne w sprawie proponowanej dyrektywy, która wkrótce powinna zostać przyjęta.

[35] Zespół reagowania na incydenty komputerowe (CERT-UE) w instytucjach UE.

[36] Ma powstać w połowie 2016 r.

i związanych z tym usługach, w rezultacie takich inicjatyw użytkownicy technologii powinni być lepiej chronieni przed zagrożeniami hybrydowymi.

<u>Działanie 12</u>: Komisja, w koordynacji z państwami członkowskimi, będzie współpracować z przemysłem w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego, by rozwijać i testować technologie mające lepiej chronić użytkowników i infrastrukturę przed zagrożeniami hybrydowymi.

4.4.2. Energia

Pojawienie się inteligentnych domów i urządzeń oraz rozwój inteligentnej sieci, co powoduje wzrost digitalizacji systemu energetycznego, powinny także skutkować większą podatnością na ataki cybernetyczne. Europejska strategia bezpieczeństwa energetycznego[37] i strategia na rzecz unii energetycznej:[38] wspierają podejście uwzględniające wszystkie zagrożenia, w którym odporność na zagrożenia hybrydowe jest zintegrowana. Sieć tematyczna dotycząca ochrony krytycznej infrastruktury energetycznej pogłębia współpracę między operatorami w sektorze energetycznym (ropa, gaz, energia elektryczna). Komisja uruchomiła platformę internetową umożliwiającą analizę i wymianę informacji na temat zagrożeń i incydentów[39]. Ponadto Komisja opracowuje obecnie, we współpracy z zainteresowanymi stronami[40], kompleksową strategię bezpieczeństwa cybernetycznego w sektorze energetycznym w odniesieniu do działania inteligentnych sieci w celu zmniejszania podatności na zagrożenia. Mimo postępującej integracji rynków energii elektrycznej, zasady i procedury postępowania w sytuacjach kryzysowych nadal mają zasięg krajowy. Musimy dopilnować, by rządy współpracowały ze sobą w zakresie przygotowania na sytuacje zagrożenia, zapobiegania zagrożeniom i ich minimalizowania oraz by wszystkie zainteresowane strony działały według wspólnych zasad.

<u>Działanie 13</u>: Komisja wyda wytyczne dla właścicieli 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.

4.4.3. Zapewnienie solidnych systemów finansowych

By móc funkcjonować, gospodarka UE potrzebuje bezpiecznego systemu finansowego i systemu płatności. Zasadnicze znaczenie ma ochrona systemu finansowego i jego infrastruktury przed atakami cybernetycznymi, niezależnie od motywu lub charakteru napastnika. Aby stawić czoła zagrożeniom hybrydowym wymierzonym w usługi

[37] Komunikat Komisji do Parlamentu Europejskiego i Rady: Europejska strategia bezpieczeństwa energetycznego – COM/2014/0330 final.
[38] Komunikat „Strategia ramowa na rzecz stabilnej unii energetycznej opartej na przyszłościowej polityce w dziedzinie klimatu" – COM/2015/080 final.
[39] Centrum UE ds. wymiany informacji o incydentach i zagrożeniach.
[40] W postaci platformy bezpieczeństwa cybernetycznego zrzeszającej ekspertów ds. energii.

finansowe UE, sektor finansowy musi zdawać sobie sprawę z zagrożeń, testować swoje środki obrony i posiadać niezbędną technologię do ochrony przed takimi atakami. W związku z tym duże znaczenie ma wymiana informacji na temat zagrożeń wśród uczestników rynków finansowych oraz z odpowiednimi organami i głównymi usługodawcami lub odbiorcami, lecz musi ona być także bezpieczna i spełniać wymogi w zakresie ochrony danych. Zgodnie z pracami prowadzonymi na forach międzynarodowych, w tym pracami grupy G-7 w tym sektorze, Komisja będzie dążyć do zidentyfikowania czynników utrudniających właściwą wymianę informacji na temat zagrożeń i zaproponuje rozwiązania. Ważne jest, aby zapewnić regularne badanie i udoskonalanie protokołów w celu ochrony przedsiębiorstw i odpowiedniej infrastruktury, w tym stałe udoskonalanie technologii podnoszących bezpieczeństwo.

***Działanie 14*: Komisja we współpracy z ENISA[41], państwami członkowskimi, 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.**

4.4.4. Transport

Nowoczesne systemy transportu (kolejowego, drogowego, lotniczego i morskiego) polegają na systemach informatycznych, które są podatne na ataki cybernetyczne. Zważywszy na swój transgraniczny wymiar UE ma do odegrania szczególną rolę. Komisja, we współpracy z państwami członkowskimi, będzie kontynuowała analizę zagrożeń cybernetycznych związanych z bezprawną ingerencją w systemy transportu. Komisja opracowuje planu działania dotyczącego bezpieczeństwa cybernetycznego dla lotnictwa we współpracy z Europejską Agencją Bezpieczeństwa Lotniczego (EASA) [42]. Ponadto zagrożenia cybernetyczne dla bezpieczeństwa morskiego stanowią przedmiot strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i jej planu działania w tym zakresie.

***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.**

[41] Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

[42] Nowe rozporządzenie w sprawie EASA jest obecnie przedmiotem dyskusji między Parlamentem Europejskim i Radą w następstwie wniosku Komisji z grudnia 2015 r. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Lotniczego oraz uchylającego rozporządzenie (WE) nr 216/2008 Parlamentu Europejskiego i Rady – COM(2015) 613 final, 2015/0277 (COD).

4.5. Działania wymierzone w finansowanie zagrożeń hybrydowych

Sprawcy zagrożeń hybrydowych potrzebują finansowania, by kontynuować swoją działalność. Finansowanie może być przeznaczane na wspieranie grup terrorystycznych lub bardziej subtelnych form destabilizacji, takich jak wspieranie grup nacisku i skrajnych ugrupowań politycznych. UE zintensyfikowała swoje działania przeciwko finansowaniu przestępczości i terroryzmu, zgodnie z Europejską agendą bezpieczeństwa, w szczególności z odnośnym planem działania[43]. W tym kontekście zmienione europejskie ramy przeciwdziałania praniu pieniędzy wzmacniają walkę z finansowaniem terroryzmu i praniem pieniędzy, ułatwiają pracę krajowych jednostek analityki finansowej (FIU), których zadaniem jest rozpoznawanie i śledzenie przypadków podejrzanych przelewów pieniężnych i podejrzanej wymiany informacji, i jednocześnie zapewniają możliwość śledzenia przekazów pieniężnych w Unii Europejskiej. Tym samym przyczyniają się one do przeciwdziałania zagrożeniom hybrydowym. Jeśli chodzi o instrumenty WPZiB, można by rozważyć zastosowanie skutecznych środków ograniczających, które byłyby dostosowane do potrzeb, w celu przeciwdziałania zagrożeniom hybrydowym.

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

4.6. Budowanie odporności w obliczu radykalizacji postaw i brutalnego ekstremizmu

Mimo że akty terroryzmu i brutalny ekstremizm nie mają same w sobie charakteru hybrydowego, sprawcy zagrożeń hybrydowych mogą docierać do najsłabszych członków społeczeństwa i ich rekrutować, prowadząc do radykalizacji ich postaw za pośrednictwem nowoczesnych kanałów komunikacji (m.in. internetowych mediów społecznościowych, „grup-przykrywek") i propagandy.

W celu zwalczania treści ekstremistycznych w internecie Komisja – w ramach strategii jednolitego rynku cyfrowego – analizuje obecnie potrzebę zastosowania ewentualnych nowych środków, z należytym uwzględnieniem ich wpływu na prawa podstawowe, jakimi są wolność wypowiedzi i informacji. Mogą one obejmować rygorystyczne procedury usuwania nielegalnych treści przy jednoczesnym unikaniu usuwania legalnych treści cyfrowych („mechanizmy zgłaszania i usuwania nielegalnych treści") oraz większej odpowiedzialności i należytej staranności po stronie pośredników w zarządzaniu swoimi sieciami i systemami. Powyższe stanowiłoby uzupełnienie obecnego podejścia na zasadzie dobrowolności, w ramach którego firmy prowadzące działalność internetową i zajmujące się mediami społecznościowymi (w szczególności w ramach internetowego forum UE), we współpracy z unijną jednostką ds. zgłaszania podejrzanych treści w internecie działającą przy Europolu, szybko usuwają treści będące propagandą terrorystyczną.

[43] Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu (COM(2016) 50 final)

W ramach Europejskiej agendy bezpieczeństwa radykalizacji przeciwdziała się poprzez wymianę doświadczeń i wypracowywanie najlepszych praktyk, w tym współpracę w państwach trzecich. Zespół Doradczy ds. Strategicznej Komunikacji w sprawie Syrii dąży do wzmocnienia rozwoju i rozpowszechniania alternatywnego przekazu w celu zwalczania propagandy terrorystycznej. Unijna sieć upowszechniania wiedzy o radykalizacji postaw wspiera państwa członkowskie i praktyków, którzy muszą wchodzić w interakcje z osobami o radykalnych poglądach (m.in. zagranicznymi bojownikami terrorystycznymi) lub osobami podatnymi na radykalizację postaw. Sieć ta zapewnia doradztwo i szkolenia oraz będzie oferowała wsparcie priorytetowym państwom trzecim, jeżeli wykażą one gotowość do zaangażowania się. Ponadto Komisja wspiera współpracę sądową między podmiotami sądownictwa karnego, w tym Eurojustem, w zakresie zwalczania terroryzmu i radykalizacji postaw w państwach członkowskich, w tym zajmowania się zagranicznymi bojownikami terrorystycznymi i osobami powracającymi.

Uzupełniając powyższe podejście w ramach swoich **działań zewnętrznych**, UE przyczynia się do zwalczania brutalnego ekstremizmu, m.in. poprzez zewnętrzne zaangażowanie i działania informacyjne, zapobieganie (zwalczanie radykalizacji postaw i finansowania terroryzmu), jak również poprzez działania mające zaradzić podstawowym czynnikom gospodarczym, politycznym i społecznym, które sprzyjają rozkwitowi grup terrorystycznych.

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

4.7. Zacieśnienie współpracy z państwami trzecimi

Jak podkreślono w Europejskiej agendzie bezpieczeństwa, UE kładzie większy nacisk na budowanie zdolności w ***krajach partnerskich*** w sektorze bezpieczeństwa, m.in. wykorzystując powiązania między bezpieczeństwem a rozwojem oraz dbając o to, by zmieniona europejska polityka sąsiedztwa w większym stopniu uwzględniała kwestię bezpieczeństwa[44]. Działania te mogą także sprzyjać większej odporności uczestników na działania hybrydowe.

Komisja zamierza w dalszym ciągu pogłębiać wymianę informacji operacyjnych i strategicznych z krajami objętymi procesem rozszerzenia oraz z państwami Partnerstwa Wschodniego i południowego sąsiedztwa w stosownych przypadkach, by pomóc przeciwdziałać zorganizowanej przestępczości, terroryzmowi, nielegalnej migracji i handlowi bronią strzelecką. W dziedzinie walki z terroryzmem UE zacieśnia współpracę z państwami trzecimi w drodze bardziej zaawansowanych rozmów i planów działania.

[44] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, przegląd europejskiej polityki sąsiedztwa, 18.11.2015 r., JOIN(2015) 50 final.

Unijne instrumenty finansowania zewnętrznego mają na celu budowę sprawnie działających i odpowiedzialnych instytucji w państwach trzecich[45], które są warunkiem wstępnym skutecznego reagowania na zagrożenia bezpieczeństwa i zwiększenia odporności. W tym kontekście kluczowa jest reforma sektora bezpieczeństwa i budowanie zdolności na rzecz bezpieczeństwa i rozwoju[46]. W ramach Instrumentu na rzecz przyczyniania się do Stabilności i Pokoju[47] Komisja opracowała działania na rzecz wzmocnienia odporności na zagrożenia cybernetyczne i zwiększenia zdolności partnerów do wykrywania ataków cybernetycznych i cyberprzestępczości i reagowania na nie, dzięki czemu może przeciwdziałać zagrożeniom hybrydowym w państwach trzecich. UE finansuje działania w zakresie budowania zdolności w krajach partnerskich, aby ograniczyć ryzyko dla bezpieczeństwa związane z kwestiami CBRJ[48].

Ponadto zgodnie z kompleksowym podejściem do zarządzania kryzysowego, by wspomóc partnerów w rozwijaniu ich zdolności, państwa członkowskie mogłyby zastosować narzędzia i misje przewidziane we wspólnej polityce bezpieczeństwa i obrony (WPBiO), niezależnie od stosowanych instrumentów UE lub jako ich uzupełnienie. Można by rozważyć następujące działania: (i) wspieranie łączności strategicznej, (ii) wsparcie doradcze dla kluczowych ministerstw narażonych na zagrożenia hybrydowe; (iii) dodatkowe wsparcie w zakresie zarządzania granicami w sytuacji wyjątkowej. Można rozważyć dalszą synergię między instrumentami WPBiO i bezpieczeństwem; organami celnymi i organami wymiaru sprawiedliwości, w tym odnośnymi agencjami UE[49], Interpolem i europejskimi siłami żandarmerii, zgodnie z ich kompetencjami.

<u>Działanie 18</u>: 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.

---

[45] Tamże; komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Strategia rozszerzenia UE", 10.11.2015 r., COM(2015) 611 final. komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Zwiększenie wpływu unijnej polityki rozwoju - Program działań na rzecz zmian", 13.10.2011 r., COM(2011) 637 final.

[46] Wspólny komunikat „Budowanie zdolności na rzecz bezpieczeństwa i rozwoju - Umożliwienie partnerom zapobiegania kryzysom i zarządzania nimi" (JOIN(2015)17final).

[47] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 230/2014 z dnia 11 marca 2014 r. ustanawiające Instrument na rzecz przyczyniania się do Stabilności i Pokoju, Dz.U. L 77 z 15.3.2014 r., s. 1.

[48] Poruszone kwestie obejmują monitorowanie granic, zarządzanie w sytuacji kryzysowej, pierwsze reagowanie, nielegalny handel, kontrolę wywozu produktów podwójnego zastosowania, nadzór nad chorobami i ich kontrolę, forensykę jądrową, przezwyciężanie skutków incydentów oraz ochronę obiektów wysokiego ryzyka. Z państwami trzecimi można wymieniać się najlepszymi praktykami zaczerpniętymi z narzędzi opracowanych w ramach planu działania UE w obszarze CBRJ, takimi jak Europejski Ośrodek Szkoleń w zakresie bezpieczeństwa jądrowego oraz udział UE w międzynarodowej grupie roboczej ds. monitorowania granic.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

5. ZAPOBIEGANIE KRYZYSOM, REAGOWANIE NA NIE I PRZEZWYCIĘŻANIE ICH SKUTKÓW

Zgodnie z pkt 3.1 zadaniem zaproponowanej komórki UE ds. syntezy informacji o zagrożeniach hybrydowych jest analiza odpowiednich wskaźników w celu zapobiegania zagrożeniom hybrydowym i reagowania na nie, a także informowania unijnych decydentów. Chociaż można minimalizować słabe punkty dzięki długoterminowym strategiom na szczeblu krajowym i unijnym, w perspektywie krótkoterminowej konieczne jest zwiększenie zdolności państw członkowskich i Unii do zapobiegania zagrożeniom hybrydowym, reagowania na nie i przezwyciężania ich skutków w sposób szybki i skoordynowany.

Zasadnicze znaczenie ma szybkie reagowanie na zdarzenia spowodowane przez zagrożenia hybrydowe. W tym kontekście ułatwianie krajowych działań na rzecz ochrony ludności i rozwoju zdolności przez Europejskie Centrum Koordynacji Reagowania Kryzysowego[50] mogłoby stanowić skuteczny mechanizm reagowania w przypadku tych elementów zagrożeń hybrydowych, które wymagają ochrony ludności. Można to osiągnąć, stosując inne mechanizmy reagowania UE i systemy wczesnego ostrzegania, w szczególności współpracując z centrum sytuacyjnym ESDZ w zakresie zewnętrznego wymiaru bezpieczeństwa oraz z centrum analizy strategicznej i reagowania w dziedzinie bezpieczeństwa wewnętrznego.

Klauzula solidarności (art. 222 TFUE) dopuszcza działanie Unii, a także działania między państwami członkowskimi, jeżeli państwo członkowskie jest przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej bądź katastrofy wywołanej przez człowieka. Działanie Unii mające pomóc państwu członkowskiemu jest realizowane w drodze decyzji Rady 2014/415/UE[51]. Uzgodnienia dotyczące koordynacji w ramach Rady powinny opierać się na zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych[52]. Zgodnie z tymi uzgodnieniami Komisja i Wysoki Przedstawiciel (w obszarach swoich kompetencji) określają odnośne instrumenty unijne i przedkładają Radzie wnioski dotyczące decyzji w sprawie środków wyjątkowych.

Artykuł 222 TFUE dotyczy również sytuacji, w których jedno lub kilka państw członkowskich udziela bezpośredniego wsparcia państwu członkowskiemu, które doświadczyło ataku terrorystycznego lub katastrofy. W tym przypadku decyzja Rady 2014/415/UE nie ma zastosowania. Ze względu na niejasności związane z działaniami hybrydowymi Komisja i Wysoki Przedstawiciel powinni ocenić ewentualne zastosowanie – jako ostateczność – klauzuli solidarności (w obszarach swoich kompetencji), jeżeli państwo członkowskie UE jest narażone na poważne zagrożenia hybrydowe.

---

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.

[51] Decyzja Rady 2014/415/UE w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności, Dz.U. L 192 z 1.7.2014, s. 53.

[52] http://www.consilium.europa.eu/pl/documents-publications/publications/2014/eu-ipcr/

W odróżnieniu od art. 222 TFUE, jeżeli wiele poważnych zagrożeń hybrydowych stanowi zbrojną agresję przeciwko państwu członkowskiemu UE, można powołać się na art. 42 ust. 7, by zapewnić odpowiednie i terminowe reagowanie. Szeroko zakrojone i poważne objawy zagrożeń hybrydowych mogą również wymagać ściślejszej współpracy i koordynacji z NATO.

Państwa członkowskie zachęca się, by w trakcie przygotowywania swoich sił zbrojnych uwzględniły potencjalne zagrożenia hybrydowe. Aby być gotowym do szybkiego i skutecznego podejmowania decyzji w przypadku ataku hybrydowego, państwa członkowskie muszą regularnie prowadzić działania, na poziomie operacyjnym i politycznym, by przetestować zdolność do podejmowania decyzji na szczeblu krajowym i międzynarodowym. Celem byłby wspólny protokół operacyjny między państwami członkowskimi, Komisją i Wysokim Przedstawicielem, określający skuteczne procedury, które należy stosować w razie zagrożenia hybrydowego, od wstępnej fazy identyfikacji do końcowej fazy ataku, i opisujący rolę każdej instytucji Unii i każdego podmiotu zaangażowanego w ten proces.

Jako ważny element zaangażowania WPBiO, mogłoby to zapewnić: a) szkolenia cywilne i wojskowe, b) misje związane z mentoringiem i doradztwem w celu zwiększenia bezpieczeństwa i zdolności obronnej państwa, któremu grozi atak hybrydowy, c) planowanie awaryjne w celu rozpoznawania sygnałów o zagrożeniach hybrydowych i wzmocnienia zdolności w zakresie wczesnego ostrzegania, d) wspieranie zarządzania kontrolą granic w sytuacjach kryzysowych, e) wsparcie w obszarach specjalistycznych, takich jak minimalizowanie ryzyka CBRJ i ewakuacja osób nieuczestniczących w walkach.

<u>Działanie 19</u>: 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.

<u>Działanie 20</u>: 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.

<u>Działanie 21</u>: 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.

6. ZACIEŚNIENIE WSPÓŁPRACY Z NATO

Zagrożenia hybrydowe stanowią zagrożenie nie tylko dla UE, lecz także dla pozostałych głównych organizacji partnerskich, w tym Organizacji Narodów Zjednoczonych (ONZ), Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), a zwłaszcza NATO.

Skuteczne reagowanie wymaga dialogu i koordynacji zarówno na poziomie politycznym, jak i na poziomie operacyjnym między organizacjami. Dzięki zacieśnieniu współpracy między UE i NATO organizacje te byłyby lepiej przygotowane i skuteczniej reagowałyby na zagrożenia hybrydowe w sposób wzajemnie się uzupełniający i wspierający, w oparciu o zasadę uczestnictwa, przy jednoczesnym poszanowaniu autonomii decyzyjnej każdej z tych organizacji i zasad ochrony danych.

Obie organizacje mają wspólne wartości i stoją w obliczu podobnych problemów. Państwa członkowskie UE i sojusznicy NATO oczekują od swoich organizacji wsparcia, sprawnych, zdecydowanych i skoordynowanych działań w razie kryzysu, a w idealnej sytuacji – zapobiegania wystąpieniu kryzysu. Zidentyfikowano szereg obszarów wymagających ściślejszej koordynacji i współpracy między UE a NATO, takich jak orientacja sytuacyjna, łączność strategiczna, bezpieczeństwo cybernetyczne, zapobieganie kryzysom i reagowanie na nie. Należy pogłębić trwający nieformalny dialog między UE i NATO na temat zagrożeń hybrydowych w celu synchronizowania działań obu organizacji w tym obszarze.

Przy opracowywaniu uzupełniających planów reagowania UE/NATO ważne jest, aby obie organizacje miały ten sam obraz orientacji sytuacyjnej przed kryzysem i w jego trakcie. Jest to możliwe dzięki regularnej wymianie wspólnych analiz i zdobytych doświadczeń, ale również dzięki bezpośrednim kontaktom między komórką UE ds. syntezy informacji o zagrożeniach hybrydowych a komórką NATO ds. zagrożeń hybrydowych. Równie ważne jest rozwijanie wśród tych organizacji wzajemnej znajomości procedur zarządzania kryzysowego stosowanych przez każdą z nich w celu zapewnienia szybkiego i skutecznego reagowania. Odporność można wzmocnić poprzez zapewnienie komplementarności w ustanawianiu wspólnych norm na tym samym poziomie w odniesieniu do krytycznych elementów ich infrastruktury, a także poprzez ścisłą współpracę w zakresie strategicznej komunikacji i cyberobrony. Wspólne działania, zakładające udział wszystkich stron, zarówno na poziomie politycznym, jak i technicznym, zwiększyłyby skuteczność obu organizacji w zakresie podejmowania decyzji. Rozważenie dalszych możliwości w zakresie szkoleń pomogłoby osiągnąć porównywalny poziom wiedzy fachowej w najważniejszych obszarach.

<u>Działanie 22</u>: 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.

7. KONKLUZJE

W niniejszym wspólnym komunikacie przedstawiono działania, które mają pomóc przeciwdziałać zagrożeniom hybrydowym i budować odporność na szczeblu UE i państw członkowskich, a także partnerów. Jako że główny nacisk położono na **pogłębianie wiedzy**, proponuje się ustanowienie specjalnych mechanizmów wymiany informacji

między państwami członkowskimi oraz koordynowanie zdolności UE do osiągnięcia łączności strategicznej. Nakreślono działania mające na celu **budowanie 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. W każdym z tych obszarów ważnym pierwszym krokiem będzie wdrożenie uzgodnionych strategii przez UE i państwa członkowskie, a także pełne wdrożenie istniejących przepisów przez państwa członkowskie, przy czym przedstawiono już pewne bardziej konkretne działania w celu dalszego wsparcia tych wysiłków.

W odniesieniu do **zapobiegania zagrożeniom hybrydowym, reagowania na nie i przezwyciężania ich skutków** proponuje się zbadanie możliwości zastosowania klauzuli solidarności zapisanej w art. 222 TFUE (jak określono w odnośnej decyzji) oraz w art. 42 ust. 7 TUE w razie wystąpienia poważnego ataku hybrydowego o szerokim zasięgu. Można by poprawić zdolność do podejmowania strategicznych decyzji poprzez ustanowienie wspólnego protokołu operacyjnego.

Wreszcie, proponuje się **zintensyfikowanie współpracy** i **koordynacji między UE i NATO** w zakresie wspólnych wysiłków na rzecz przeciwdziałania zagrożeniom hybrydowym.

W trakcie wdrażania przedmiotowych wspólnych ram Wysoki Przedstawiciel i Komisja angażują się w mobilizowanie stosownych instrumentów UE będących do ich dyspozycji. Ważne jest, by UE wraz z państwami członkowskimi dążyła do zmniejszenia ryzyka związanego z narażeniem na potencjalne zagrożenia hybrydowe ze strony podmiotów państwowych i niepaństwowych.